



PHARE PROGRAMME TWINNING PROJECT NO. LV/2002/IB/OT-01
DATA STATE INSPECTION

Document 28

Activity 4.4

Data Protection in the Social Welfare Administration

Brochure for Data Protection officials within social welfare institutions

written by

Nils Leopold, Theresa Philippi

August 2005



**Ludwig Boltzmann Institut für Menschenrechte
Mandated Body**



DATU VALSTS INSPEKCIJA

This publication has been produced with the assistance of the European Union. The contents of this publication can in no way be taken to reflect the views of the European Union.

Social welfare administrations process huge amounts of personal data. Eligibility for state benefits today usually requires the disclosure of a wide range of personal information by the applicant. Social welfare systems and its benefits and contributions run by the state usually distribute the money of the taxpayers. These services and benefits mostly are delivered without a particular consideration by the receiving persons. Citizens thus expect their governments to take strong measures against the obtainment of these financial funds e.g. by fraud. Particular problems arise from the fact that some instruments of social welfare like for instance social services and social assistance are delivered on the basis of a close evaluation of a persons actual need and resources. This may lead to almost all-embracing collections of the personal data of the person involved. Additionally the responsible administrations tend to process the given data for numerous purposes like internal revisions etc. in order to optimize or to guarantee a more effective allocation of their funds.

This situation may conflict with the rights of the citizens to the protection of their personal data. The right to the protection of one's own data has been acknowledged as a fundamental and often even constitutionally guaranteed right in most modern nations in the world. The constitution of the European Union guarantees the right to data protection in Article II – 68.

The EC Data Protection Directive 46/95 that already has come into force in 1998 regulates possible conflicts and draws the basic structure and content of the citizens' rights to data protection. It will probably soon be implemented by a revised Latvian data protection law. Both laws fully apply to the data processing within the field of social welfare administration. Its provisions have to be respected and be brought to full effect by the responsible authorities and their management. Failures to adapt these regulations may lead to arduous appeals procedures and – due to the given legal regulation – even law suits or public notice by way of the national data protection authority.

The following sections give an outline of basic principles that will have to be taken into account when establishing a data protection regime or even a management system within social welfare administrations. It will focus on Latvian social services, social assistance and social insurance which have been monitored on the basis of their legal regulations.

Importance of Data Protection in social welfare systems

Social security measures serve as to implement social rights that aim at realizing a dignified and autonomous life of EU citizens. Both aspects - the protection of human dignity and the protection of the autonomy of the individual in various facets – are reflected in the charter of fundamental rights of the European Union. When realizing data protection rights it should be taken into account that the basic normative goals are identical. Those citizens striving, applying or heavily relying on social security measures deserve full recognition of their citizens rights both in terms of actual financial support and in *terms of procedure* when their personal data they submit in order to receive support are being processed. It should be kept in mind that those in need of social care support may expect at least the same standards of data protection as other citizens. The particular character of data processing in the field of

social security as well as the types of data involved *even speaks for a stronger protection regime*. This has been acknowledged by some member states years ago: National legislators have amplified the primary list of sensitive data in the sense of Article 8 EC-Directive by a whole series of very different data. A second, equally characteristic example is the references to social security data as, for instance, contained in both Greek and Swiss law. The wording of the Danish and the Icelandic law is broader. Instead of addressing social security they speak of data related to "social problems". What they mean, however, is information related to the support provided in economically, physically and psychologically critical situations. But even in countries in which, as in Germany, the law has up to now deliberately renounced enumerating sensitive data, the processing of social security data is subject to a markedly restrictive regime. Few other barriers are as high as "social secret". The background is the same everywhere. To the extent that individual risks are socialised, the transparency of individual behaviour increases. The condition for providing support is an ever growing amount of data meticulously depicting both the problems and the general situation of the data subjects. Where therefore social security systems are institutionalised and continuously expanded, the data they process quickly reach the top of the sensitivity scale.¹

As long as there has no sector - specific legislation been introduced this goal should be realized by extensive interpretation of those legal provisions leaving a wide discretion for the weighing of interests at stake.

Operational and organisational structures in welfare administration have a significant own interest in upholding a strong data protection regime: especially social services and social assistance systems heavily rely on mutual trust of the participating sides. Those who have to reveal their full economic and social situation to the government are in fear of being publicly stigmatized or excluded from public life. They take a particular interest in the confidential processing of their data. The social support for families and especially children or the processing of data about disabilities or mental diseases may serve as a good example.

In all these cases personal information are prerequisites for the understanding and evaluation of the need for individual support. *Effective administrative measures cannot be taken without the trusting support of the individuals involved delivering information about their true situation. Therefore it becomes clear that in the field of social welfare administration data protection serves as a self-evident prerequisite of the effective supervision of the social welfare system as a whole.* This trust can be won by assuring that the often highly sensitive data (like for instance medical data) and information given by the persons concerned are being kept in a safe environment, are being processed within the bounds of law and are being kept confidential.

¹ Simitis, Revisiting sensitive data, 1999, see

Main Principles of the protection of social data

Responsible Data controllers and legal instruments reviewed

Social data meaning all personal data being processed by institutions carrying out social security and social welfare measures will fall within the scope of the directive and the Latvian Data protection law from 23 March 2000. These institutions include

- local government social service offices
- ministry of welfare
- state social services agency
- other social service providers
- State medical examination commission
- Social care council
- State employment agency
- State occupational career choice agency
- Work placement agencies
- Doctors, psychiatrists, social workers
- All institutions dealing with calculation and deliverance of State social insurance benefits and other benefits, compensations or pensions

These institutions are all for themselves legally responsible in upholding the data protection provisions. It should be clarified that within local governments in terms of personal data processing there should be separate divisions with separated filing systems and data banks depending on the given task that is being carried out (like for instance social service offices or unemployment reduction divisions).

Social data protection encompasses all data processing when working with the following known² legal instruments:

1. Benefits, compensations and pensions as listed by the state social insurance agency³
2. Law on social services and social assistance from 2003
3. Social security against unemployment, law passed 2002

Scope of the Directive

Personal data encompasses all information relating to an identifiable person. Persons remain identifiable as long as the information given about them open for the possibility of retrieving their full name. Merely pseudonymous registers or filing systems will therefore fall within the scope of the directive.

In the context of social security and social welfare systems a subset of these personal data can be categorized as sensitive in the meaning of the EC-Directive: they include information about for instance the health status or even the sexual life of persons and therefore deserve a particular high level of protection. This holds especially true for a number of benefits being offered like childbirth benefits, sickness or disability benefits, but also for certain compensations and pension entitlement (for more on sensitive data see below).

² Project experts results on the bases of internet research carried out on location, August 2005-08-05

³ <http://www.vsaa.gov.lv/vsaa/content/?lng=en&cat=704>

It is also important to note that the *EU Acquis* encompasses all personal data that are part of a filing system characterized by its retrievability. As a consequence, the already existing paper files also have to be treated according to data protection rules as long as they are accessible according to specific criteria (e.g. alphabetical principle of arrangement).

The core of the problem in Latvia: The concept of sensitive data and social welfare systems

All personal data revealing information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life in principle should not be processed at all.

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

However, the EC-Directive opens up for flexible national regulations in some cases (Article 8 para 2 b. for employment law; Article 8 para 3 management of health care services), as long as it is authorized by national law providing for adequate safeguards or - in the case of health data - these data are being processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy *or by another person also subject to an equivalent obligation to secrecy.*

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national

competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

Moreover, in recital No 34 to the Directive seemingly the whole area of social protection is exempt from the prohibition of processing of sensitive data as long as there is an important public interest justifying it and specific and suitable safeguards to protect the fundamental rights and the privacy of the individuals are being taken:

34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

Finally, recital 22 of the data protection directive rules that

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

and Article 5 underlines that

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

These provisions do leave member states certain discretion in defining the safeguards for the persons affected. However, as long as there aren't any additional sector-specific regulations protecting sensitive data in Latvia, in accordance with the *acquis communautaire*, it should be noted that at least with respect to the directives requirement of a special protection for sensitive data, legal measurements have to be taken.

It is fair to say that from the *acquis communautaire*, which also encompasses the traditions and practices in other member states, at least the following suggestions for immediate changes can be made until the legislator will meet its legal obligation for further regulation:

- All social welfare instruments inducing the collection and processing of sensitive data should be registered by the data protection officer of the responsible institution

- The collection process should take into account that sensitive data should not be collected at all unless it is absolutely necessary for the performance of the explicit task
- The particular subset of sensitive information should be listed in advance and the specific purpose for which they are needed and are being processed should be explicitly documented
- The transmission of these data to other entities or institutions should be prohibited unless it is unavoidable in order to realize for the performance of the purpose of the task
- Technical and organizational measures should secure that these data are being kept apart from the other social data and that only staff actually involved in the specific decision process gain access to these data
- The staff involved needs, in addition to their official duties and commitments to secrecy and confidentiality, should receive further training instructions by their supervisors on the non-disclosure/non-dissemination of these data. The actual performance of the training should be documented.
- The citizens affected should at least receive the information listed in Article 10 of the Directive (identity of the controller, purpose of processing, recipients of categories of the given data, rights of data subjects affected)

It is advisable as to survey whether the whole range of social data (all personal data being processed for the purpose of social welfare and social security by social administrations) should receive the protection level as sketched above. In some member states particular *social security secrecy* in connection with sector-specific rules upholds and maintains a confidentiality regime for all officeholders and other persons involved in the processing of social data. This bears a clear advantage of not having to establish a system of double standards in trying to identify and to process sensitive data which will most probably be found in many of the social security instruments like benefits, compensations or pensions implying certain sensitive data for application processes.

Social security administration and the duty to inform after Article 10

Many of the above listed Latvian social security measures include provisions about what information has to be presented by the data subject in order to receive funding or support. In these cases of course it is known to the data subject which personal data have been delivered to which authority and for what purpose. According to Article 10 of the EC-directive in these cases it therefore will be suitable to only give further information after Article 10 c., in so far that this seems necessary with regard to the specific circumstances of the data collection and the need to guarantee a fair processing of the data.

(c) any further information such as

- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

This will for example be of special importance when personal data of the data subjects are transmitted to an authority (e.g. for specific registers) which is not mentioned in the legal bases for the state benefit or support that the individual had applied for.

Particular attention should be taken to the need to inform the data subject on their right to object to data processing after Article 14 (see also below).

The duty to inform after Article 11

As soon as complex social welfare structures are growing being intertwined in multiple ways and allowing for multiple transmissions of data through digitalized network structures it becomes ever more important to adopt the provision of Article 11 in a reasonable manner. On the hand the data subject has a full right to know where his data have been collected and stored. On the other hand data subjects are in need of few but precise descriptions not confusing them on the actual location of their data.

It is suggested to review the existing data transmission structures especially in the area of social insurances on whether additional data from other institutions and registers are being collected and added to the decision process on certain benefits without the data subject actually being able to know this. It should be checked then, how within the decision process a reasonable information, perhaps as an integral part of form sheets for example, an information meeting the requirements of Article 11 can be given.

Strict purpose binding principle and necessity principle to be applied in social welfare administration

Article 6 and 7 of the EC-directive form the cernel of data protection in social welfare administration. Taking into account the often great numbers of at least partly highly sensitive data being processed in this field it is absolutely vital to guarantee the rights of the individuals by applying Article 6 and 7 strictly:

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

This leads to the obligation of the data controllers to define and advisably to put down in writing in advance the purpose for which the data are being processed as precise as possible. It should be kept in mind that the term processing of data encompasses all possible variations:

Example: The responsible social welfare administration pays benefits or regular amounts of funding by transferring the money on the bank accounts of the citizens receiving support. It should be part of a professional data protection management

and in accordance with the *EU acquis communautaire* to prevent the disclosure of the purpose of the transaction to third parties during the communication process (e.g. towards postal services or the bank of the person concerned).

Any change of purpose has to be checked whether it can be legitimated after the same provisions. Typical processing like statistics for controlling purposes or for future budgetary planning etc need additional appropriate safeguards. Many member state countries have implemented this by keeping the processing pseudonymous or even anonymous by consequently cutting off all identifiers from the data being used.

The legitimating principle after Article 7 EC-Directive typically will involve the following provisions:

- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Example: After the law on social services and social assistance there will be social workers taking care of children and their families and providing psychosocial assistance to them. All information on the situation of single individuals, for instance information on criminal records should be kept confidential. It should be information left to deal with for the responsible social worker only. It is also prohibited for the (state) institutions involved to build up local criminal record registers of the children they are taking care of since this would be an illegal database built on excessive collection of data not needed for handling the single case. This would also be in conflict with the proportionality principle as laid down in Article 6 of the EC-Directive.

Principle of accuracy after Article 6 d of the EC-directive

All personal data stored within social welfare administration permanently needs to be monitored and reviewed in regard to their correctness and actuality. Data protection rules require management processes within each responsible authority to ensure the accuracy of the data in order to avoid decision taking on the bases of false data.

- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

The data subjects rights after Article 12 of the EC-directive

Article 12
Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

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

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

These rights often have been referred to as the “magna charta” of data protection. This serves as to hint at the fundamental importance of transparency and individual knowledge about one’s own data. Only the individuals’ full knowledge about the extent of the ongoing data processing opens up for further steps to be taken: the right of rectification, erasure or blocking of personal data cannot be exercised without the knowledge about the ongoing practice of processing. Law suits against ongoing pretended illegal data processing also heavily rely on the amount and quality of information about the data being processed. Therefore all responsible data controllers in the field of social welfare administration should be aware of and establish an internal regulation on what section holds the responsibility for answering to possible inquiries made by the citizens concerned.

Particular attention should be given to Article 14 a. of the Directive. The right of the data subject to object - on compelling grounds - to the processing of data relating to him or her is a rather strong instrument for data subjects as long as there aren’t any sector-specific rules in national legislation leading to its exclusion. This situation may also serve as an argument for further sector-specific regulation in the field of social welfare administration. Currently there aren’t any rules excluding this possibility for the citizens concerned.

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Data transfers to foreign countries

Due to the goal of the EC-directive to harmonize the level of data protection in the member states in order to allow for a free flow of personal information, the possibility of the transfer of social welfare data between EU-countries and to third countries should be mentioned.

Example: The Latvian social insurance agency suspects a citizen to receive income related social funding not just here but also from Germany. They file a request to the German colleagues.

While harmonization has led to the possibility of a free flow of information between institutions exclusively carrying out tasks in the field of social welfare, the general rules for data transfers to other entities/authorities will apply when other administrations are concerned.

Data transfers to third countries remain legally problematic. Probably the only solid foundation will be a bilateral agreement with the receiving nation including provisions on the processing of the data involved.

Article 16 and 17 of the EC-Directive

The fact that huge amounts of personal have to be processed in the course of social welfare administration leads to the need for service providers (data processors). The transfer of data to these entities has to be secured by organizational and technical means. A number of measures have to be taken in order to guarantee the confidentiality of the data. Illegal access effectively needs to be hindered. Specific contracts with the service provider form the legal grounds for the transfer of the personal data. The minimum requirements of these contracts in terms of data protection are outlined in Article 16 and 17.

Organizational and technical measures have to be taken by all responsible controllers in order to prevent the personal data from being destroyed. Typical measures include regular data storage processes on a physical carrier (e.g. CDs and other).