



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

Document 23

Activity 4.2
**Development of an awareness strategy for data
controllers and processors**

written by

Univ.-Prof. Dr. Dietmar Jahnel

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.

The general purpose of this activity is the development of an awareness strategy for data controllers and processors in general concerning their rights and obligations according to EU and Latvian data protection laws and the role and function of the DSI (respectively the Data Supervisor). The aim of the strategy is to act as a basis for activity 4.3: Creation of material for an awareness campaign among data controllers and workshops/training for data controllers. Therefore the differences in an awareness strategy especially for controllers and processors in public security authorities will only be outlined in form of a short statement at the end of this paper.

First of all it is necessary to give an overview of the obligations, the controllers and processors have to observe. After that a short outline of the role and function of the DSI (respectively the Data Supervisor) is provided as far as controllers and processors are concerned. Step three will consist in the proposal of several specific activities which can be followed to raise the awareness for data protection of data controllers and processors.

1. Obligations controllers have to observe

In an awareness campaign for data controllers it will not make sense just to copy the terms of the Latvian and European laws. It should be achieved to explain the sometimes very complicated regulations of the data protection laws in an easy way understandable to everybody. Examples should be given to illustrate the regulations whenever possible.

a) Criteria for making the processing of data legitimate

- Criteria for making the processing of personal data legitimate (Section 7 PDP-law; Art 7 EU-directive): the most important criteria are the unambiguously given consent of the data subject, the necessity for the performance of a contract and the necessity for the purposes of the legitimate interests pursued by the controller or by a third party.

- Criteria for making the processing of sensitive personal data legitimate (Section 11 PDP-law; Art 8 EU-directive): it should be explained that the processing of sensitive personal data is prohibited unless one of certain exceptions are fulfilled.

b) Notification

- Obligation to notify the supervisory authority (Section 21 PDP-law; Art 18 EU-directive): it should be explained where and how the processing system has to be notified, the exceptions of the notification and where the forms for the notification can be found.

c) Information to be given to the data subject

- Information in cases of collection of data from the data subject (Section 8 PDP-law; Art 10 EU-directive)
- Information where the data have not been obtained from the data subject (Section 9 PDP-law; Art 11 EU-directive): it has to be explained what kind of information has to be given to the data subject under which conditions.

d) Confidentiality and security of processing

- Confidentiality of processing (Section 27 PDP-law; Art 16 EU-directive): the controller is responsible that natural persons involved in personal data processing make a commitment in writing to preserve and not disclose personal data in an unlawful manner.
- Security of processing (Section 25 PDP-law; Art 17 EU-directive); the controller has to implement appropriate technical and organizational measures (such as use of passwords or special documentation) to protect personal data against destruction or unauthorized disclosure or access.

e) Response to the data subject's right of access to data

- Response to the right of access (Section 15 PDP-law; Art 12 EU-directive): the controller has to provide information as to who processes what data concerning the data subject, where the data originated, for

which purpose they are used and to whom the data are transmitted within a period of one month and free of charge.

- Response to the right of rectification, erasure or blocking of data (Section 16 PDP-law; Art 12 EU-directive): the controller has to rectify or erase data that are incorrect or unlawful by his own, as soon as he becomes aware of that fact or on an application by the data subject.

- Response to the right to object (Section 16/2, 19 PDP-law; Art 14 EU-directive): the data subject has the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him.

2. Role and function of the Data Supervisor

According to Section 30 (1) PDF-law the Data Supervisor advises and controls all administrative bodies, as well as all private parties in matters of personal data protection.

Every person, also every public official, may directly contact the Date Supervisor or his staff.

The Data Supervisor registers personal data processing systems and cancels a certificate of personal data processing registrations, if violations of law are established.

If the Data Supervisor finds that personal data processing regulations have been violated in a particular case by a public institution he is provided with a wide range of methods of intervention (Section 30 (2) PDP-law).

The Data Supervisor may order private persons to process, block, erase or destroy data, impose a temporary or definite ban on processing, or impose fines on private persons for violations of personal data protection rules according to the penal code. Administrative decisions by the Data Supervisor concerning private persons may be appealed against to the administrative courts by the person concerned.

3. Proposals for specific activities

First of all it has to be taken in account that in general data controllers regard data protection as a hindrance and as a cost factor. Therefore the idea that data protection can also be a positive factor in competition as customers are increasingly knowledgeable about their rights and prefer companies which honor these rights, must be transmitted to business circles. This factor will become more and more important when Latvian companies will increase their trade with other EU-member states and states outside the EU in the future.

Inside the EU there are no restrictions to transmission of data to recipients in other member states, even if this may not be justified by the actual situation in a specific member state. Therefore it will be necessary for all data controllers in Latvia involved in international commerce to gain the same level of data protection as the rest of the member states.

When an awareness campaign is prepared it is important to keep in mind that the implementation of new rights and obligations requires a certain amount of time. In countries like Austria and Germany data protection laws are in force for more than 20 years. In the beginning the awareness for data protection was very low in the general public as well as with data controllers. A wide discussion of this matter started only several years ago with the use of e-mail and internet by employees, with the growing importance of electronic commerce, in connection with the start of electronic government and recently because of the increase of video surveillance.

a) Awareness campaign for data controllers and processors in general

Teaching of data protection officials:

According to the new section 23 of the PDP-law public and private bodies which process personal data automatically may appoint a data protection official. When the controller has appointed a data protection official, the personal data processing operations are exempt from the notification requirement (Section

21/3/6 PDP-law). It can be foreseen that this will be a big incentive for data controllers to actually appoint a data protection official.

As only persons who possess the specialized knowledge and demonstrate the reliability necessary for the performance of the duties concerned may be appointed data protection official, it will be necessary to establish a data protection curriculum for people who are interested to apply for this position. In this curriculum the rights and obligations of the data controllers and processors have to be explained and examples could be given how certain types of data protection relevant situations have been dealt with in Latvia so far, in other member states of the EU and by the European law court.

This will be probably the most effective and cost efficient way to raise the awareness for data protection.

Written information material:

For data controller who do not appoint a data protection official as well as for the data protection officials themselves written information material should be prepared. This information material should provide general knowledge about the obligations of data controllers and processors as listed above in chapter 1. It seems very important to emphasize that this material has to be written in a way that is highly understandable to persons who had no contact at all with data protection before.

The production of information material in print and for download in the World Wide Web is the aim of activity 4.3.

Webpage:

The World Wide Web is an easy and very cost effective way to provide information on data protection for controllers and processors and for the general public.

The webpage of the DSI (respectively the Data Supervisor) should cover the following aspects:

- General information on data protection as a fundamental right and on data protection regulation in a comprehensive form.
- Information on the specific rights and obligations of the data controller as listed in chapter 1. An example of how these rights and obligation may be explained can be seen on the Austrian site www.help.gv.at / Unternehmer/in / DVR.
- A very effective way to provide information is to collect the questions asked by data controllers and to publish the answers as so called FAQ (frequently asked questions).
- A very important part could also be an example form on how to give information about the processed data.
- Information on the rights of the data subject.
- Specific information for the lawyer as a consultant of the data controller in cases concerning data protection law. This section should provide:
 - All relevant data protection regulations (Latvian and European).
 - Decisions of the DSI (respectively the Data Supervisor).

An example of such a webpage can be seen at the site of the Austrian Data Protection Commission at www.dsk.gv.at/.

In Germany a lot of information material about data protection can be found at www.datenschutz.de. But this site is an example that too much information can mean no information at all: At the section “folders, leaflets ...” several hundred (!) documents can be found, and these documents are not systematized but listed in alphabetical order. Even someone interested in data protection is not willing to scroll through this entire list to find the information he is looking for.

At last one disadvantage of this media has to be mentioned: Information on a website is considered so called “pull”-information, which means that the person who is looking for information has to be aware of the problems concerned and play an active role to obtain the information he is looking for. Therefore the

website can act as an information platform only for those data controllers, who are already aware of the importance of data protection.

e-learning platform:

The internet can even be utilized in a much more advanced way. The state electronic data processing center (“Bundesrechenzentrum”) of Austria has developed an e-learning platform on the topic of data protection. The employees are given the possibility to learn the basic principles of data protection using this intranet application in the form of self-study. At the end of the session a multiple choice test is available to verify the result of the lessons.

This concept was created to raise the awareness concerning data protection of all employees of the Austrian state electronic data processing center. More information on “e-learning data protection” can be obtained at Johannes.mariel@brz.gv.at.

Teach the teachers:

The awareness campaign for data controllers should also include the scientific community in Latvia as stated in the strategy for an awareness campaign for the general public (activity 4.1). The juridical faculties respectively universities in Latvia should be approached to gain their support not only for a “kick-off-meeting” introducing the idea of data protection to a selected public, but also to achieve that data protection law and special cases will be discussed amongst law teachers and lawyers.

Lawyers must become aware of the fact that there is a wide field for consultation and publication in matters concerning data protection, regarding topics such as internet-provider, e-shops, data in social security, data in public security authorities and so on. The same is true for law teachers.

Publication of administrative decisions by the DSI (respectively the Data Supervisor):

Administrative decisions of the DSI (respectively the Data Supervisor) have to be published in the World Wide Web for general access at no costs. This is one of the fundamental requirements to achieve that the jurisprudence will deal with data protection cases and everybody interested in the topic of data protection can have a look at decision in real cases. Only examples may show the relevance and importance of data protection in real life.

Media activity:

The importance of Media activity was already emphasized in activity 4.1. The same is true for the awareness strategy for data controllers and processors.

b) Awareness campaign for data controllers and processors in public security authorities

For data controllers and processors in public security authorities Section 12 of the PDP-law is relevant: Personal data, relation to criminal actions, previous convictions in criminal cases shall only be allowed for processing by persons and in cases provided by the law. A complete register of criminal convictions may be kept only under the control of official authority.

For the development of an awareness strategy for this target group the obligations the controllers have to observe are to be found in the specific law which regulates the rights and obligations of public security authorities. Therefore chapter 1 of this awareness strategy has to be adopted according to the specific regulations, which have not been translated into English up to now.

It must be considered that appropriate measures to protect personal data and internal security precaution make it a lot easier to direct an authority. For the director of an authority it is essential to regulate the competences and responsibility for processing of personal data. The proposals of specific activities for an awareness campaign (see chapter 3) basically keep the same.