



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

Document 10

Final Report on Activity 1.3
Preparation of Comments on the Latvian data protection
legislation

written by
Elisabeth Duhr
Prof.Dr. Nikolaus Forgó

Summer 2005



Ludwig Boltzmann Institut für Menschenrechte
Mandated Body



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.

1. Objective of the Activity and Overview

The objective of the Activity 1.3 of the present Phare Twinning Project is the preparation of a commentary on the Latvian legislation explaining unclear and vague terms in the law on the base of the case law on the European Court of Justice and the European Court of Human Rights as well as the most significant decisions of German and Austrian Courts in selected areas.

2. General Remarks on the Latvian Personal Data Protection Law

The commentary of the regulations of the rights of a data subject is based on the version of the Latvian Personal Data Protection Law (further: PDP law) in force as of 20 November 2002, last amended 24 October 2002 and on the Electronic Communications Law in force as of 1 December 2004. The amendment of 2002 of the Latvian Personal Data Protection Law was necessary with view to the access of the Republic of Lithuania to the European Union, which was effected in May 2004. This version of the PDP law reflects some changes regarding compliance with the Directive 95/46/EC. Thus, the regulations of Section 15, 17 and 18 were amended. This report includes a commentary on the general principles for personal data processing as stated in Section 7 of PDP law and a commentary on the data subject's right as stated in Section 15 to 20 of PDW law. The provisions lay down fundamental requirements to be met by any processing of personal data. The corresponding articles of the Directive 95/46/EC and the respective recitals are added in this report.

The commentary is designed to become a working tool for everybody who has to deal with questions regarding interpretations of the mentioned regulations. The basis of the work was the official English translation of the PDP law as published on the website of the DSI and the translation of the Electronic Communications Law made available on the website of the Tulkošanas un terminoloģijas centrs (www.ttc.lv).

PDP law - General Principles for Personal Data Processing

Section 7

Personal Data processing is permitted only if not prescribed otherwise by law, and at least one of the following conditions exist:

- 1) the data subject has given his or her consent;**
- 2) the personal data processing results from contractual obligations of the data subject or, observing request of the data subject, the data processing is necessary for conclusion of the corresponding contract;**
- 3) data processing is necessary to a system controller for performance of his/her obligations established in the law;**
- 4) data processing is necessary to protect vitally important interests of the data subject, including life and health;**
- 5) data processing is necessary in order to ensure that the public interest is complied with, or to fulfil functions of public authority for whose performance the personal data have been transferred to a system controller or transmitted to a third person; and**
- 6) data processing is necessary in order to, complying with the fundamental human rights and freedoms of the data subject, exercise lawful interests of the system controller or of such third person as the personal data have been disclosed to.**

Directive 95/46/EC

Section II – Criteria for making data processing legitimate

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or*
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or*
- (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).*

Recitals:

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

Remarks on the Directive

Art. 7 of the Directive presents the core provision defining the general rules which must be met to regard a data processing as lawful. The provision includes a concluding enumeration binding on all Member States. Additional requirements for a processing of personal data are stated in Art. 6 of the Directive. The processing of special categories of data is defined in Art. 8 of the Directive. The Member States have to transpose these provisions into national law. In doing so, there is a certain margin; the Member States are not obliged to completely exhaust the scope predefined by Art. 7. However, if they create more restrictive regulations, they shall not hinder the free flow of personal data between Member States.¹

Comments to PDP law

According to the first clause of section 7 processing of personal data is prohibited unless one of the regulations specified in the PDP law or in other regulations applies. Exceptions to this prohibition must be explicitly provided for having regard to specific requirements acknowledging the fundamental freedoms and privacy of a data subject in accordance with the state constitution. By checking data processing operations the question has to be asked whether one of the following regulations applies or whether a sector-specific regulation exists. If not, the data processing operation is illegal.

¹ Cf. Dammann/Simits, EG-Datenschutzrichtlinie, Kommentar, Art. 7, para. 2.

Pursuant to Section 2 (1) consent of a data subject shall mean a freely, unmistakably expressed indication of the wishes of a data subject by which the data subject allows his or her personal data to be processed according to information delivered by a system controller in compliance with Section 8 of PDP law. Consent has to be asked before the start of data processing. The data subject shall be informed of the name and address of the system controller and of the purpose of the personal data processing in an adequate manner. The information provided by the system controller shall enable the data subject to overview the significance of his consent. There is no regulation in regard to the form of the consent. But it is advisable for the system controller to ask for consent in writing in order to prove consent has been given by the data subject. If consent is to be given together with other written declaration it should be made distinguishable in its appearance to avoid non-observance by the data subject. Consent has to be given by the data subject in person.

No consent has to be given in case the processing of personal data is compatible with the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject according to Section 7 (2). If processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, processing of personal data is permitted. For example, to fulfill rights and duties of an insurance contract or a bank contract personal data related to the contract have to be collected, recorded, transmitted and so on. Basic principle for any processing operation related to a contract is the need for the specific personal data. Restriction to necessary data is based on the principles of a constitutional state permitting infringements of human rights and freedoms only in respect of specific needs. Collecting of personal data ahead and in excess or of data being only useful, not restricted to the respective purpose, is therefore illegitimate.

Pursuant to Section 7 (3) processing of personal data is permitted if a statutory obligation or a legal provision applies, for example, processing of personal data pursuant to Law on Police, processing pursuant employment law or keeping of a register according to Latvian law.

According to the provision of Section 7 (4), processing is regarded as lawful where it is carried out in order to protect an interest, which is essential for the data subject's life. It has to be asked in this context if the processing should even be legitimate if it does not meet the approval of the data subject. If the data subject is incapable (physically or legally) to give his consent, processing shall be legitimate under the specified circumstances. But if the data subject is capable to give consent this should be asked and processing should not be carried out defying his decision. Decision of the data subject has to be respected.

The provision of Section 7 (5) referring to public bodies is restricted to the needs of the specific purposes. Public bodies are not allowed to collect, record, use and so on more data as actually needed in each individual case. Assessment criteria thereby must be strictly observed. Public bodies shall not – under false pretences – process more data than necessary. By assessing legality of data processing operations of public bodies it has to be considered that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The purposes for which the data are to be processed or used shall be specified in concrete terms prior to the collection of the data. Otherwise public bodies could, as they think best, change the purposes afterwards. Such a proceeding would be incompatible with the principles of the Directive and those of a constitutional state. The data must be adequate, relevant and not excessive to the purposes for which they are

collected and /or further processed. If these requirements are not complied with the processing is unlawful.

The provision of Section 7 (6) primarily is addressed to private bodies. Processing of data is lawful if processing is necessary for the purposes of the legitimate interests pursued by the system controller or by the third party to whom the data are disclosed, and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. In each individual case the interests of the system controller and the data subject have to be balanced in order to assess the legality of data processing. The interests of the system controller or third party shall comply with the Latvian legislation and state constitution. Illegitimate interests of the data subject, for example concealing crucial facts related to creditability, must not be considered.

PDP law - Rights of a Data Subject

Section 15

(1) In addition to the rights mentioned in Sections 8 and 9 of this Law, a data subject has the right to obtain all information that has been collected concerning himself or herself in any system for personal data processing, unless the disclosure of such information is prohibited by law in the sphere of national security, defence and criminal law.

(2) A data subject has the right to obtain information concerning those natural or legal persons who within a prescribed time period have received information from a system controller concerning this data subject. In the information to be provided to the data subject, it is prohibited to include State institutions, which administer criminal procedures, investigation operations or other institutions concerning which the disclosure of such information is prohibited by law.

(3) A data subject also has the right to request the following information:

- 1) the designation, or name and surname, and address of the system controller;**
- 2) the purpose, scope and method of the personal data processing**
- 3) the date when the personal data concerning the data subject were last rectified, deleted or blocked;**
- 4) the source from which the personal data were obtained unless the disclosure of such information is prohibited by law; and**
- 5) the processing methods utilised for the automated processing systems, concerning the application of which individual automated decisions are taken.**

(4) A data subject has the right, within a period of one month from the date of submission of the relevant request (not more frequently than two times a year), to receive the information specified in the Section in writing free of charge.

Directive 95/46/EC

Section V – The data subject’s right of access to data

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.

Section VI - Exemptions and restrictions

Article 13

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

Recitals:

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

Remarks on the Directive

The Directive 95/46/EC lays down a number of principles that contain the fundamental requirements to be met by any processing of personal data. The data subject's rights are central to any data protection system as they are the primary means to assert one's "right to informational self-determination". The Directive includes a 3-step model of information: First of all the data subject has to know that there has taken place a processing of his personal data, second, he has to be informed which personal data were processed and third, if the results of the processing significantly affect him, he has the right to obtain knowledge of the logic involved in the automatic processing of data to allow the data subject to check the process and comment on possible mistakes in the process.

The provision of Article 12 shall assure that the right to access his own personal data is not turned against the data subject. Especially the case that a service is offered by the recipient under the condition of giving away personal data by the data subject while the direct transfer to the final recipient would have been illegal has been seen as a major problem of circumvention.

Further conditions shall secure a free and unconstrained access to its personal data. Delay or cost for example may not be used against the data subject while exercising its

right. On the other hand there shall be no misuse by data subjects through excessive use of its rights, why free access has to be given not in a permanently ongoing manner but just in reasonable intervals.²

Art. 13 Dir. includes several exemptions from the principle of information and transparency. According to Art. 28 (4) Dir. the data subject has a right to ask the supervising authority to check legitimacy of processing in cases where complete transparency was not given according to one of the enumerated exemptions. For the background of the exemption see Recital (43).

Comments to PDP law

Section 15 subsection 1 defines the data subject's basic right of access to data. On request of the data subject, the system controller has the obligation to provide all information that has been collected concerning the data subject. The data subject's right to know about the processing of his personal data corresponds with the general principle of transparency (see also Recital 38 of the Directive). The right of access to data is of particular importance among the rights of a data subject. Data subject's rights are central to any data protection system as they are the primary means to assert one's "right to informational self-determination". To exercise informational self-determination, the data subject moreover requires knowledge on which personal data is processed and the possibility to act on its informed decision. Therefore the right of access and the right to object are important further parts of the legal protection of the data subject's rights.

The Directive provides in Art. 13 for a number of exceptions relating to major public interests for several provisions on the two conditions that such exemptions must be provided for in "legislative measures" and be "necessary", i.e. respect the proportionality principle, among others, to safeguard the public interest. Therefore, Section 15 subsection 1 of PDP law defines exceptions to restrict the right of access in case the disclosure of the information is prohibited by law in the sphere of national security, defense and criminal law. The restriction of the right of access has to be specified in the respective regulations.

The provisions of Section 15 subsection 2 state the right of a data subject to obtain information about all recipients to whom the data are disclosed from the system controller. The scope of this right is restricted to the information of recipients to whom the data were disclosed within a prescribed time period. The meaning of the restriction is unclear and must therefore be interpreted in consideration of the respective regulations of the Directive. Art. 13 of the Directive states no exemptions or restrictions of the right of access for a specified period of time. Thus, the right to access extends to all processed data relating to the data subject. Restriction to a prescribed time period in Section 15 subsection 2 of PDP law violates the Directive and is irrelevant.

The information to be provided to the data subject shall not include information about State Institutions that administer criminal procedures, investigating operations authorities or other institutions concerning such data, if so regulated by law. The restriction of the right of access transposes Art. 13 (1) d of the Directive.

Section 15 subsection 3 specifies the content of information. The system controller must provide a data subject with information on the identity of the system controller, i.e. name and address. The identity requirement is fulfilled, if a unique identification of the data

² Compare Ehmann / Helfrich, EG-Datenschutzrichtlinie: Kurzkommentar, 1. ed., Cologne 1999, Art. 12, 19.

