



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

Document 7

Activity 1.2

The directive 95/46/EC as superior law to the national law

written by

Dr. Tino Naumann

December 2004



**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.

1. The directive 95/46/EC¹ as superior law to the national law

On 1 May 2004 the Republic of Latvia joined the European Union. Already by signing the Association Agreement in 1995,² Latvia had undertaken to transpose the full *acquis communautaire* into national law. Considering that, it can be concluded that Directive 95/46/EC is setting out the basic standard of the *acquis communautaire* for personal data protection and being the principle source of the supranational law in the field for the Republic of Latvia.

Yet, by the country's accession to the EU, a new dimension was added. According to established jurisprudence by the European Court of Justice (ECJ), certain provisions of the EC Treaty, or even a directive, may develop direct effect, provided that they are sufficiently clear, unconditional, and the time limit for their transposition into national law has expired. Furthermore, according to the *Francovich* judgment,³ Member States can be held liable for failing to transpose a directive within the prescribed deadline.

Furthermore according to Art. 226 of the Treaty establishing the European Community⁴ the European Commission will launch infringement procedures against Latvia for failure to implement or for implementing incorrectly the directive in national law.

What does independence mean?

The Directive unmistakably speaks of ... complete independence in exercising the functions entrusted to them.⁵

As mentioned above the unambiguous rule of the directive which stands above the national law shall be transposed into Latvian law.

A real Data Protector may be very annoying to the executive power and its highest representatives if his concern is of political impact or becomes the latter during the control or reproof procedure. It is known from experience as well as a current pattern of behaviour that the law permanently obstructs the political leadership by supporting the adherence of competence, fair and clear procedures, open, comprehensive and court proof justifications instead of subliminal arguments in the case decisions are made by "informal administrative assistance" and by the using of silent and plain information flow, pseudo-justifications and superior knowledge.

Everyone who keeps politics on the legal track in the described manner will become unpopular soon. This is valid in clearly arranged ergo personnel interwoven societies and is even more valid if a part of the media and therefore the publicity is politically bound or vice versa isolated by politics.

Every institution, including huge private enterprises as well as complex public structures, the state power or political parties, uses to tend to qualify or neutralise all those who endanger the procedures or their objects (or the leader in the crowd). All those who act due to legal regulations or approved rules of conduct contrary to patterns of behaviour of

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

² Europe Agreement establishing an Association between the European Communities and their Member States, of the one part, and the Republic of Latvia, of the other part [1998] OJ L 26/3.

³ Joined Cases C-6/90 and C-9/90 *Andrea Francovich et al. v. Italian Republic* [1991] ECR I-5357.

⁴ consolidated version, Official Journal C 325 , 24 December 2002

⁵ Directive 95/46/EC (supra, fn 1), Art. 28.1.

their organisation - regardless of their basis and influence – will be noticed as a disturbing factor, neutralised and replaced by a person who seems to be compatible to the system. I.e. a somewhat independent Data Protector might be thwarted.

This danger to the constitutional state must be prevented by a clear-cut guarantee of a institutional independence i.e. independence with regard to contents, organisation and the person of the Data Protector. Because the executive power of the State and the other public bodies are the main objects of the Data Protector's control, he must be completely independent of the Cabinet of Ministers. The directive says that the data protection supervising authority must "act with complete independence in exercising the functions entrusted to them". This is meant to emphasize that that they must not only be given formal independence from all subjects of control but must also be free from any interference in practice.

Although no single formula exists, a number of elements do contribute to safeguarding independence. Such elements include:

- the composition of the authority,
- the method for appointing its members,
- the office term and conditions for dismissal,
- the allocation of sufficient resources to the authority, and
- the power to take decisions completely free from any external influence.

These elements are also mentioned in the explanatory report to the additional protocol to Council of Europe Convention 108/81.

Factual independence means not only independence from current majorities. Furthermore the data protector must not be influenced by any third party. (Only) the affected data subject or the affected public or private body shall have the right to take legal action against a decision made by the data protector.

Therefore shall be no supervision at all, neither a legal supervision i.e. such as instructions what, who, how deep someone might be controlled by who nor a factual supervision concerning i.e. the legitimacy of the chosen procedure or the decision itself.

There must be a disciplinary supervision provided by law. The latter must not narrow the independence of the Data Protector as it is granted to judges and covers i.e. the course of business, the appearance of handling of business or issues not covered by the factual field of functions (i.e. accounting, employment of staff, working hours).

Consequently only the Chief Justice of the Supreme Court or alternatively the Speaker of the Saeima shall be entitled to initiate a disciplinary matter.

Functional independence traditionally consists of ultimate jurisdiction for budget, staff, interior administration, acquisition of material and public relation.

The budget is provided for by a certain law that does contain appropriate sections for the President, the administration of the Saeima, the Auditors General and the Supreme Court et cetera. Consequently the budget of the Data Protector shall be provided for also in an appropriate section. The Data Protector shall draft his budget and transfer it to the Saeima.

The Data Protector is the disciplinary supervisor to his staff. He appoints and releases his staff by applying the according law.

Presumably the staff will not exceed the number of 30 members. Therefore the interior administration and the acquisition of material might be combined with another authority as long as his independence of the Data Inspector is not affected.

One of the most important duties of the Data Protector is to inform the public. As a matter of course he must not disclose state secrets and must protect the right of personality and trade secrets of a third party. He shall fulfil this duty on his own responsibility.

Current situation in Latvia

Article 95 and 96 of the *Satversme* (Latvian Constitution) provide, respectively:

95. The State shall protect human honour and dignity. Torture or other cruel or degrading treatment of human beings is prohibited. No one shall be subjected to inhuman or degrading punishment.

96. Everyone has the right to inviolability of their private life, home and correspondence.⁶ While these provisions protect human dignity and privacy in general, data protection more particularly is addressed in the Law on Personal Data Protection (further: "PDP Law") of 23 March 2000), which came into force on 2 January 2001.⁷ Since its adoption, the Law has been amended once – on 24 October 2002.

Based on the PDP Law, a "Data State Inspection" (further: "DSI") was created. The DSI is charged with and empowered to supervise and control the observance of the PDP Law in general,⁸ review complaints,⁹ certify data commissioners,¹⁰ register personal data processing systems,¹¹ carry out inspections,¹² order that data be blocked, and that incorrect or unlawfully obtained data be erased or destroyed,¹³ impose fines and/or other administrative sanctions for violations of the PDP Law,¹⁴ and bring actions in Court for violations of the PDP Law.¹⁵

The basic framework is thus in place, but does not ensure full compliance with Directive 95/46/EC. Certainly, more than passing a few basic laws and setting up a data inspection is required. In order to meet the requirements of the *acquis communautaire*, it is necessary that (a) every single provision of the directive be accurately transposed into Latvian law, and (b) the adapted legal provisions are properly implemented in Latvia.

The one aspect of overriding importance in which the Latvian PDP Law clearly does not measure up to the standard of the *acquis* is the independence requirement with regard to the supervisory authority.

Section 29 of the Personal Data Protection Law provide, respectively:

⁶ Constitution of the Republic of Latvia (*Satversme*) 1922 (8 May 2003) - Latvijas Vēstnesis, nr. 43, 01.07.1993. Available on the internet (in English translation) at: <http://www.satv.tiesa.gov.lv/Eng/satversme.htm>.

⁷ "Fizisko personu datu aizsardzības likums" of 23 March 2000 - Latvijas Vēstnesis, nr. 123/124, 06.04.2000.

English translation (consolidated version) available on the internet at: <http://www.dvi.gov.lv/eng/legislation/pdp/>.

⁸ Arts. 29(1) and 29(3)1.

⁹ Art. 29(3)2.

¹⁰ Art. 29(3)6.

¹¹ Art. 29(3)3.

¹² Arts. 29(4)1, 2 and 7.

¹³ Art. 29(4)3.

¹⁴ Arts. 29(4)5 and 6.

¹⁵ Art. 29(4)4.

(1) Supervision over personal data protection shall be carried out by the State Data Inspection which shall be under jurisdiction of the Ministry of Justice, The State Data Inspection shall be an institution of state administration, The State Data Inspection shall be managed by a director who shall be appointed and released from his or her position by the Cabinet pursuant to the recommendation of the Minister for Justice.
(2) The State Data Inspection shall act in accordance with by-laws approved by the Cabinet. ...

Also on that point the commission made its standpoint clear as follows:

“The Commission expects that, where necessary, Member States will amend their legislation to achieve compliance with the provisions of the Directive and provide supervisory authorities with sufficient resources. The Commission also expects that Member States and supervisory authorities will make all reasonable efforts to create an environment in which data controllers – and not least those operating on a pan-European level and/or international level – can conform with their obligations in a less complex and burdensome way and to avoid imposing requirements that could be dropped without any detrimental effects for the high level of protection guaranteed by the Directive.”¹⁶

¹⁶ First report on the implementation of the Data Protection Directive (95/46/EC), page 27