



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

Document 4

Final Report on Activity 1.2
Preparation of recommendations and proposals for the
improvement of the Latvian data protection legislation

written by

Professor Dr. Marie-Theres Tinnefeld

July 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. Introduction

The European Community does not have as a goal merely the achievement of a Single Market. The vision of a unified Europe entails the growing together of the European nations that in the long run would develop a European Citizen's mindset. The use of information technology can assist the transfer of information and knowledge. It can carry further the administrative and economic development in the European countries. The national and European legislator must take into account the information and communication technology and prepare the building of a common legal framework required for the **information society**. The citizens in all Member States of the European Union need equal protection of their **basic rights**.

In administrative and economic life there is a substantial need for the basic material „personal data“. A multitude of information data about everyone will be processed, transferred across borders and combined with numerous other data. This development points to the importance of the **protection of personal data** (the right to privacy).

Every instance of processing personal data in principle infringes on the individual's right to inviolability of private life, home and correspondence, as stated in Article 96 of the Latvian Constitution. Therefore, restrictions of that right must have a legal basis (see Art. 116, Latvian Constitution). Exact regulations are furthermore important for the citizens, whose rights are restricted by law. This is a constitutional principle, which can be derived from the democratic principle embodied in Article 1 of the Constitution of Latvia. Clear and exact regulations are necessary for the data processing institutions and for the data subject. Especially there should be an independent Data Supervisor, because personal data are typically processed without the knowledge of the data subject.

2. Objective of the Activity and Remarks

The objective of Activity 1.2 has been the drafting of recommendations and proposals for the improvement of the Latvian data protection legislation. The following remarks deal with the current legal provisions concerning the independence of the national supervisory authority for personal data protection, as well as with the procedure for

notification and registration of personal data processing systems according to the Latvian Personal Data Protection law (PDP law). The report also deals with the new provisions as embodied in the draft amendment to the Latvian PDP law, which was produced as a result of the present Phare Twinning project. The compatibility of these provisions with Directive 95/46 EC of the European Parliament and of the Council (in the following: the Directive) has been analysed to identify potential shortcomings of the PDP law.

The report starts with an overview of the current situation (3). The subsequent remarks deal with the proposals of the short-term experts and the proposal by Dr. Thomas Giesen und Marcis Gobins to amend the PDP law with a focus of an independent data supervisor (4). This leads to proposals for further amendments to the PDP law, which include the definition of an informed consent, as well as special regulations in the areas of scientific research and freedom of media (5).

3. Overview

All highly developed European states nowadays protect the right to privacy, also referred to as the right of personal data protection. The Latvian Constitution has expressed this right into Article 96, which is identical to Article 8 ECHR – „Everyone has the right to inviolability of their private life, home and correspondence”. As a basic right that is entrenched in the Constitution, this right is applicable to the legal relations between the individual and the State, as well as between two individuals. Insofar, there is no conflict to the European data protection Directive, which is also applicable to both the public and the private sector.

The Latvian legislator has so far incompletely transferred the Directive into the Latvian PDP law. Notably, there are deficiencies in the area of informed consent (which constitutes a legal basis for the processing of personal data in a number of cases). Furthermore, the problem of personal data protection in the media is incompletely covered, and the problem of personal data protection in research is not at all covered by the Latvian PDP law. These shortcomings shall be discussed in more detail in section 5 of this report.

The transfer of personal data inside and outside of the European Community is a further particular problem area. Firstly, the Latvian PDP law, which was written at a time when Latvia was not yet a member of the European Union, should now no longer differentiate between data transfers within Latvia, on the one hand, and international data transfers, on the other. As an EU Member State, Latvia should draw the principal line of division between data transfers within the EU, and such transfers that involve third countries outside of the EU (see our proposal for a new Section 28 para 5, further). Moreover, although the present Latvian legislation may not yet measure up to the requirements of the Directive in this area, individual appliers of the law may already assume that there is a sufficient standard of data protection in all EU Member States (in reality, the existence of an equal standard of protection throughout the EU is fictitious). In practice, this means that there is no obligation on Controllers to check the standard of protection prior to transferring personal data to other EU Member States (e.g. outsourcing).

Given this, it should nonetheless be kept in mind that the EC is bound to initiate infringement procedures to ensure that the Directive is transposed, as necessary. As a matter of fact, the **European Commission** has already warned that it might have to initiate an **infringement procedure against the Republic of Latvia, if the Directive will not be fully transposed** (see letter by Mr. Renaudière of 1 December 2004). If the Latvian legislator would fail to act in the present situation, this might lead to liability proceedings against the Republic of Latvia.

In the following, we will analyse the main shortcomings of the Latvian legislation with regard to the material as well as the procedural provisions of European data protection law. The German Constitutional Court has pointed out in its famous Census decision (*Volkszählungsurteil*) of 1983 that because of the continuous and rapid development of automated (nowadays: digital) data processing technologies, a pre-emptive protection of personal data protection is required, which should be carried out by independent institutions (BVerfGE 65, 1, 46).

In the same way, the *acquis communautaire* requires an early pre-emptive protection of personal data protection rights in addition to the reactive protection of these freedom rights by the Courts. This is even more important in view of the fact that the data subject often is unaware whether, how and for which purpose his data are processed. The

national supervising authorities for personal data protection shall act with complete independence in exercising the functions entrusted to them, and shall be subject to the law only – Directive, Article 28 para 1). The supervising authority's position outside of the general administrative hierarchy is indispensable for its ability to effectively protect individual rights against political or societal pressures. The need to establish and strengthen an independent institution was accordingly a special focus of Activity 1.2 of the present Phare Twinning project.

According to the Directive (Art. 18 para 1-4) there is no duty to notify electronic personal data processing systems with the data supervisor if certain preconditions are met. In particular, this is the case where the controller has appointed a data protection official. The notification/registration procedure does neither apply to non-automated data processing systems (Art. 18 para 5 Directive).

In addition to this, the effectiveness of freedom rights may be ensured by appointing a data protection official (Section 18 para 2 second sub-paragraph of the Directive). By appointing a knowledgeable and reliable data protection official as an instance of self-control in personal data protection matters notification/registration requirements can be minimised. The system of self-control, if implemented in a similar way as in the German Federal Data Protection Act, can be very effective and cost-efficient for processors above a certain minimum size. It is well-suited to further a reduction of bureaucracy and to flexibly combine strict data protection standards with up to date technical solutions (see Art. 17 para 1 of the Directive).

Furthermore, the European data protection *acquis* offers possibilities of self-regulation for sectoral associations, or for multinational companies, which makes sense as a practical solution for large companies that operate across borders while sharing one corporate legal culture. Notably, self-regulation is quite popular in European countries such as the Netherlands, as well as in non-European countries such as the United States.

The progress of data protection law depends to a great extent on the progress of the information technology, which does not recognise national, European or global borders. For this reason, the IT industry (and other industries, as appropriate) should develop

self-regulatory mechanisms in specific areas and work out „codes of conduct“, or „legal industrial standards“.

4. Proposals and Amendments to the Latvian PDP law

In the framework of the present Phare Twinning project, the short-term experts Dr. Schnoor, Dr. Wippermann, Dr. Naumann from Saxony and Ms Duhr from Hamburg have elaborated draft amendments to the Latvian PDP law, to fully transpose the Directive into Latvian law, in particular, with regard to the independence of the supervisory authority for personal data protection, as well as with a view to simplify the present notification/registration procedure.

On the basis of these preparatory works, the RTA, Dr. Giesen, and his Assistant, Mr Gobiņš, produced a **final draft amendment to the Latvian PDP law**, which was discussed with and **approved by Deputy State Secretary Ms Juhansone of the Ministry of Justice**. Some of the key provisions of this draft will be discussed in the following.

4.1 The Data Supervisor

4.1.1 Independence

The Data Supervisor's power to act with complete independence in exercising the functions entrusted to him is ensured by election by Parliament (*Saeima*) on nomination by the President of the Constitutional Court. He is accountable to the *Saeima*.

4.1.2 Profile of the Data Supervisor

The Data Supervisor has to be a person who is well versed in law and in technical matters. Knowledge of supranational and international law is also desirable. This is of importance because the Data Supervisor represents Latvia in European and international bodies in the area of personal data protection. Language skills should be a precondition here, too.

4.1.3 Reporting

The Data Supervisor has to produce and publish an annual report; it is recommended that this report should be presented to the *Saeima*. Everyone should have access to this report. The Data Supervisor's report is one of his sharpest weapons, although personal names should be anonymized therein as far as possible. The anonymisation in the annual report is without prejudice to the right of the Supervisor to highlight gross individual violations of privacy in the media by calling names of real persons or legal persons.

4.1.4 Term of office

To further strengthen the Data Supervisor's independence, a ten-year term is foreseen in the draft amendment, with no possibility of re-election. Alternatively, a six-year term with a one-time possibility of re-election may be considered. The Data Supervisor's salary, which is the same as that of the Auditor General, as well as to appropriate social and retirement guarantees are meant as supplementary provisions to support his independence. Furthermore he is not entitled to have any other income. These securities are intended to reinforce the office in view of temptations of corruption.

4.1.5 Limits to the Data Supervisor's competences with regard to the media

The present wording of the Latvian PDP law already protects the media from undue interference or controls by the Data Supervisor with independent journalist reporting. The media must be able to work free from any State influence in order to fulfil their essential functions as watchdogs of democratic rights. Nevertheless, internal controls of the media might be recommendable (see chapter 5.4 of this report).

4.2 Exemptions from registration duties

The Directive permits a number of exemptions from the duty to notify data processing systems with the Data Supervisor in certain cases. The Latvian PDP law so far did not make full use of these possibilities offered by the Directive, thus unnecessarily complicating the DSI's work. The draft amendment (Art. 21 paras 3 and 4) provides for a number of new exemptions from notification, in line with the Directive, some of which are presented in the following.

4.2.1 Exemption for small scale processing

Data processing systems may be exempt from the duty to notify personal data

processing systems to the Data Supervisor on condition that the controller processes personal data for his own purposes, a maximum of twenty employees are concerned with the processing of personal data, and either consent has been obtained from the data subject, or the processing serves the purposes of a contract or a quasi-contractual fiduciary relationship with the data subject (Art 21 para 3 sub-para 1 of the draft amendment).

Small-scale processors of personal data may appoint a data protection official, although this would be voluntary provided that the above criteria are met, according to the draft amendment.

4.2.2 Data protection officials as institutions of self-control

Article 17 of the Directive provides for the appointment of data protection officials as an alternative to external supervision and controls. Reliable and competent data protection officials make it possible to simplify the notification/registration systems and thus avoid “data cemeteries” (see Art. 21 (1) 6 and Art. 22 of the draft amendment). This is an efficient way to minimise administrative effort and costs. The draft amendment provides that data protection officials may be appointed in the public as well as in the private sector. The draft amendment moreover foresees that the controller must inform the Data Supervisor of the name of the data protection official.

4.3 Simplification of notification formalities

The draft amendment provides the scaling down of formalities for those data processing systems that have to be notified with the Data Supervisor (Art. 21a of the draft amendment). This is in line with the principle of a sparing use of personal data, and will help to minimize red tape and administrative burdens.

4.4 Professional associations and self-regulation

The Directive allows broad self-regulation in the area of personal data protection, especially for international enterprises. The draft amendment foresees the involvement of professional associations into the law making procedure, too. This is a first step in the way of self-regulation, as provided for by the Directive. When put into practice, it will help to create data protection provisions that would closely reflect industry or other specifics and, again, minimise administrative bureaucracy.

5. Further amendments to the Latvian PDP law

5.1 The Question of Informed Consent

The question of informed consent is regulated in Section 2 (2), 7 (1) and 8 of the existing Latvian PDP law. The present wording of these provisions does not yet fully correspond to the requirements of the *acquis communautaire*. According to the Directive, certain preconditions with regard to content and form of the data subject's consent have to be fulfilled (Art. 7 letter a of the Directive). In addition to this, German data protection law requires a written form for the consent to be valid. In any case, the data subject must be advised about legal consequences (including the purpose of processing and the responsible data controller) of their consent to a data processing operation, and this consent has to be documented. The data subject's consent must not be given under duress. A data subject's refusal to agree to processing of their data must not lead to any detrimental consequences that are in no direct relation to the sought after consent.

In the public sector, a data subject's consent must not be sought for processing operations that are unrelated to a State institution's competence. This follows from the principle that public authorities need a basis in law for all of their acting. Thus, a basis in law is the normal standard for data processing in the public sector, and the data subject's consent is an exemption.

The definition of a data subject's consent in the Latvian PDP law (Sec's 2 and 4) meets the requirements of the Directive. Yet, it would be desirable to amend it for improved clarity.

Art. 8 (in conjunction with Art. 2) of the Directive foresees that a data subject's consent to processing of their sensitive personal data must be *explicit*. The Latvian PDP law requires a written form for a data subject's consent to processing of their sensitive personal data (Sec 11 Abs. 1). However, the written form by itself is insufficient to meet the standard of the Directive which denotes that the data subject must be duly informed about the context of the intended processing of their personal data, as well as of the sensitive nature of the data to be processed.

Proposal for an amendment: Sec 11 (1):

The data subject has given his explicit written consent.

5.2 The Question of Data Transfer

The Latvian PDP law, which was written at a time when Latvia was not yet a member of the European Union, should now no longer differentiate between data transfers within Latvia, on the one hand, and international data transfers, on the other. As an EU Member State, Latvia should draw the principal line of division between data transfers within the EU, and such transfers that involve third countries outside of the EU

Proposal for an amendment to Section 28 of the Latvian PDP law:

(1) Personal data may be transferred to a State outside the European Community if that state ensures a level of data protection corresponding to the relevant level of the data protection effective in Latvia. Transfers of personal data within the European Community are treated in the same way as transfers of data within the Republic of Latvia.

5.3 The Question of Data Protection and Freedom of Science

Proposal for a science clause in the Latvian PDP law, Section 11a

Art. 113 of the *Satversme* is worded as follows:

The State shall recognise the freedom of scientific research, artistic and other creative activity.

The wording of the above constitutional provision seems to indicate that the State must not unnecessarily accroach the competence to conduct research. On the contrary, the freedom of scientific research is to be understood as an integral element of the individual freedoms. This means that researchers should be free to team up at universities, research institutes or projects to realise their right to freedom of scientific research.

Scientific research is the open-ended, systematic search for the truth. According to German Basic Law (Art. 5 Abs. 3 GG; see furthermore Art. 10 ECHR) the freedom of scientific research also extends to the free choice of methods, planning and implementation of research projects (see the following German Constitutional Court decisions: BVerfGE 35, 79, 112, 114; s.a. E 47, 327, 368). The last does however not apply to commissioned research projects. The legislator is obliged to create preconditions in law for an unhampered realisation of the freedom of research. This necessarily involves far-reaching rights to access to personal data for certain types of research. Sector specific data protection provisions apply here according to the Directive.

In practice, this means that there must be a weighing of two diverging basic rights – the right to personal data protection, on the one hand, and the right to freedom of scientific research, on the other – that must both be realised as far as possible.

In particular, historical, criminological, medical and pharmacological research can impossibly be conducted only on the basis of anonymised personal data only. The conflict between the information requirement of scientific research, on the one hand, and privacy, on the other hand, is seen especially where sensitive data are needed for research in the areas of medical health, sexuality, or criminology. The Directive in principle sanctions the processing of personal data for purposes other than the original purpose under certain strictly limited conditions (Art. 6 para 1 letter b and Art. 11 para 2 Directive).

As far as, in exceptional cases, no national provision can be applied to data processing in the area of scientific research, the data subject's consent would be required. This consent must be documented and must not be given under duress. The data subject's free will must be principal at all times. Yet, the consent does not have to be given in written form if this formal prerequisite would manifestly hamper the object of research. Professional self-regulatory sets of rules such as the Ethical Principles for Medical Research Involving Human Subjects of the Declaration of Helsinki can be helpful here, or may even be integrated into sector specific provisions of national law.

Proposal for a science clause in the Latvian PDP law, Section 11a:

Para 1. The provisions of this law are also applied to the processing of personal data for the purposes of scientific research, with the following exemptions. A data subject's informed consent to processing of his data may be granted in other than written form where the special characteristics of the research so require and the objective interest of the scientific research outweighs other interests. That being so, the considerations for waiving the requirement of a written consent are to be documented.

Para 2. As far as the purpose of the scientific research so permits, personal identifiers are to be stored separately from other research data; personal identifiers are to be deleted as soon as the purpose of the scientific research so permits.

Para 3. Personal data that are collected or stored for the purpose of scientific research must not be processed for any other purpose.

Para 4. A person or an institution that is conducting scientific research may publish personal data only in the following cases:

- 1) the data subject has expressly agreed to their publication; or*
- 2) the publication of personal data is essential for the presentation of research results in the area of contemporary history, and is not overridden by the interest of the data subject.*

Para 5. In cases where this law is not applicable to the recipient of the personal data, they may only be transferred on condition that the recipient commits to adhere to paragraphs 1-4 of this article.

Para 6. A person or an institution that is processing personal data in order to conduct scientific research, they must appoint a data protection official according to Section 22 of this law. The mandatory provision of information to anyone on request according to Section 22a of this law is limited to the information that the personal data are processed "for the purposes of scientific research". Where it is intended to process personal data for the purposes of scientific research, there is no prior checking.

5.4 Data Protection and the Freedom of Media

Section 5 Latvian PDP law:

- (1) Sections 7, 8,9 and 11 of this Law shall not apply if personal data are processed for journalistic, artistic or literary purposes, and it is not prescribed otherwise by law*

(2) In applying the provisions of Paragraph one of this Section, regard shall be had to the rights of persons to inviolability of private life and freedom of expression.

The above provision should be transferred into a new Sec 11b with necessary supplements.

The Latvian Constitution explicitly protects the freedom of expression:

“Art. 100: Everyone has the right to freedom of expression, which includes the right to freely receive, keep and distribute information and to express his views. Censorship is prohibited.”

The German Basic Law guarantees the freedom of press as well as radio and television broadcasting (Art. 5 para 1 GG), which is essential for the democratic decision-making process. Considering the fact that the processing and storage even of sensitive personal data can be of central relevance for journalistic-redactional work, Art. 9 of the Directive provides for a special derogation from standard data processing rules for the press in order “to reconcile the right to privacy with the rules governing freedom of expression”.

The effective functioning of the media is only guaranteed if the relationship between media and whistle-blowers is out of question (journalist ethics) (see BVerfGE 20, 162, 216 and E 66, 116; Decision of the ECHR Goodwin v United Kingdom, Rep. 1996-II 483, OJZ (1996), 795ff.).

Proposal for a science clause in the Latvian PDP law:

- (1) The journalist-redactional work of the media shall be unrestricted on principle. Their freedom is limited by the individual’s right to privacy which has to remain untouched in its essence. This applies without prejudice to the provisions on data security in Section 14 para 3.*
- (2) All media are obliged to appoint a data protection official. He controls all personal data processing, without prejudice to the redactional secrets.*
- (3) The Data Supervisor is not entitled to control the journalistic redactional work of the media (Sec 29 para 1). He is entitled to comment journalistic redactional work in case of an open conflict within the media.*

6. Sectoral Laws

The Directive and the PDP law are general laws, or umbrella laws. As a matter of general principles of law, sectoral norms of law are regarded as setting aside norms which are general by nature (*lex specialis derogate legi generali*). Accordingly, the provisions of the PDP law (e.g. its general provisions with regard to sensitive data, in Art. 11) will be set aside by relevant sectoral laws.

On the other hand, only where this is unavoidable, sectoral laws will apply definitions or legal terms that are different from those given in the general law. In any case, it must be kept in mind that all legal provisions should be transparent and comprehensible for data subjects, as well as for data controllers and processors both in the public and private sectors.

6.1 Electronic Communications Law

The short-term expert Dr. Naumann has scrutinized the Latvian Electronic Communications Law with regard to its compatibility to Directive 95/46/EC, as well as to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Electronic Communications Directive). He has drafted amendments and/or proposals to delete incompatible provisions of the present Latvian Electronic Communications Law, as appropriate. It is worth noting here that according to Dr. Naumann's proposal, the Data Supervisor should *inter alia* be responsible for ensuring data protection in the electronic communications sector.

In addition, it should be noted here that the data subject's **consent** to processing of his data for purposes other than those originally indicated, should not be given in the form of an opt-out-solution in written form, but rather in the form of an opt-in solution, which might also be given in the form of a secure electronic consent according to **up to date technical standards**.

At this point, we will cite the convincing argument on the thematic complex of the data subject's consent by Professor Dr. Gerling, the data protection official of the German Max-Planck-Institute:

“Telecommunication is a business where the relationship between the company (the service provider) and the customer is primarily handled using electronic communication media. Therefore, all requirements for written consent are counterproductive. It is recommended that a contract can be concluded by means of electronic communication. As regards contracts to be concluded by e-mail, the digital signature is probably the only way to do it. Unfortunately, this requires a PKI, which can work reasonably well only in closed groups (e.g. within a company). An electronic agreement on a web page can be handled much easier. A good way to do this is to require the customer to retype or reenter. If the information is presented in a way that an automatic process cannot handle (e.g. a graphic with distorted text or number unreadable to optical character recognition (OCR) systems), this is reasonably safe. In such a character or text (up to 10 characters) information (e.g. a date, a contract number) can be encoded. The procedure must ensure that the action cannot be triggered by accident (e.g. by a simple mouseclick).”

The future is likely to supply for a legal consent solution in the telecommunication sector based on even higher technical standards.

6.2 Select problems of personal data protection in the area of security (i.e. in the field of application of the Law on Police and of the Investigatory Operations Law)

6.2.1

The short-term experts Mr. Mauersberger (Office of the Saxon Data Supervisor) and Professor Dr. Paeffgen (University of Bonn) discussed the Law on Police and the current regulations in Section 15 of the Latvian PDP law in connection with the fundamental human right to privacy protection, as spelled out in the Directive and in Article 96 of the Latvian Constitution (*Satversme*). Mr Mauersberger’s main focus was the discussion of the data subject’s principal right to be informed of every instance of processing of his personal data (according to Section IV of the Directive) vis-à-vis the police, irrespectively whether his data are processed automatically or in a non-automated filing system.

In the following, Mr. Mauersberger’s **reasoning** shall be cited in excerpts:

“The claim to information on processed personal data in section 15 of the Personal Data Protection Law and its general character does not regard the special conditions of police

activities. Section 15 of the Personal Data Protection Law is a legal base to claim against public and private data controllers. Obvious there are differences between the kinds of data processed by private data controllers and different public authorities. The police bodies are allowed to utilise investigatory methods, they receive information from the office for the protection of the Constitution and they process information that may be of high importance for the public safety. Therefore a specified regulation that takes into account the peculiarity of police activities is necessary. Although the rights of data subjects should be regulated only in general data protection law to afford a clear and comprehensible legal base and a simple access to information, the special peculiarities of activities in the sphere of national security, defence and criminal law require adapted regulations. One possibility to regard the peculiarities of police activities is the integration of a regulation in the Law on Police, because the police are the relevant data controller. This could be managed with a complete regulation in the Law on Police as showed in the first proposal. Because of the indefiniteness of the current section 15 of the Personal Data Protection Law a referring regulation in the Law on Police would has to be quite detailed (see the second proposal). On the other hand it is not impossible to regulate the claim to disclosure of processed personal data in the Personal Data Protection Law (see the third proposal). In this case the data subject does not have to look for regulations in specific law. The regulation should be comprehensible (as every legal regulation). An advantage of the integration in the general data protection law is the cachet for all data controllers, private ones as well as public authorities. All public bodies are addressees of the Personal Data Protection Law. That includes the police bodies, too. The current regulation in section 15 paragraph 1 of the Personal Data Protection Law only states the refusal of the disclosure that is prohibited by law in the sphere of national security, defence and criminal law. Section 304 of the Criminal Law prohibits the disclosure of information in a pre-trial investigation without the approval of the prosecutor. The new Criminal Procedure Law contains regulations on the disclosure of criminal procedure files. As far as I can see the Law on Official Secrets do not regulate the disclosure of information or the prohibition of disclosure. Section 6 of the Law on Police states the prohibition of disclosure of information that is an official secret or other secret specifically protected by law. Furthermore the section prohibits disclosing data from a pre-trial investigation without the permission of the prosecutor or the head of the investigative institution, as well as materials that are contrary to the presumption of innocence. Another prohibition of disclosing in that section concerns information that infringes the privacy of persons or violates the honour and dignity of natural or legal persons. It is not clear, whether the legal prohibition of disclosing applies to the request of a data subject that demands information about processed personal data concerning itself. Therefore a regulation in the Law on Police (a complete regulation or a section referencing to the

general section in the Personal Data Protection Law) would clarify not only the obligation of the police to disclose processed personal data towards the data subject but the compatibility of disclosure with the prohibition of the disclosure towards third parties. The claim to disclosure information deriving from the right in Article 96 of the Constitution affects only the data concerning the data subject itself.

Data processed in a current pre-trial investigation that is lead by a prosecutor must not disclose. In those cases the data subject may appeal to the prosecutor to obtain information about the processed personal data. The right place for regulations concerning this point is the Criminal Procedure Law.

The claim to disclosure processed personal data of the data subject contains all existing information. A disclosure of data concerning only one special procedure would not be in accordance with the constitutional right of Article 96 of the Constitution. The police stores data and information in several data bases, which are described in a (administrative) regulation for every data base. In these regulations prescriptions concerning disclosure for data subjects can be found, as a representative of the police mentioned. The information centre of the ministry of the interior administrates the police data bases. According to the information of the police representative, the data subject could claim access to the processed personal data in the information centre. A legal base for this procedure was not mentioned. The data stored in the mentioned data bases administrated by the information centre of the ministry of the interior are covered by the claim to disclosure as well, because these data are processed by the police, too. In the case that the police are not allowed to disclose information stored in the data bases, the police are obliged to point out the possibility to claim disclosure of personal data in the information centre.

The disclosure of data the police received from other authorities which fulfil tasks in the sphere of national security, defence or protection of the Constitution depends on the consent of such authorities. In these cases the police are not allowed to refuse the request of the data subject without an own request to the authority that provided the data. Then the data providing authority has to examine, whether it would be obliged to disclose the regarding information.

In some cases the disclosure of information might endanger the public security or predominant interests of third persons that are involved in the administrative actions. Although the right to know, which data are processed by State authorities, is a constitutional right, it always is to be seen in interaction with other affected rights and interests. If other important rights or interests are endangered by a disclosure of

information, the police are obliged to deny a request. Nevertheless the data subject still is a person with constitutional rights. The decision denying a request of disclosing collected personal data affects the data subject in its constitutional right stated in Art. 96 of the Constitution and must be reasoned. If the reasoning is impossible without a disclosure of information that endangers important state interests or interests of third persons, the information denying body must not found its decision but it must refer to the possibility to appeal to the data protection board. The data protection board must be entitled to examine the circumstance and to obtain all information that allows an examination of lawfulness of the data processing. Although the data protection board controls the lawfulness of the data processing, it is not allowed to disclose information in communication to the data subject.“

6.2.2 Reasoning about the Personal Data Protection of the Latvian Security Authorities

The short time experts Mr. Mauersberger and Professor Dr. Paeffgen have convincingly argued that the protection of the right to one's privacy, home and correspondence (Art. 96 of the *Satversme*) is of high importance even vis-à-vis the legitimate interest of the State to an effective prevention of threats to public order and security, or to an effective criminal law enforcement.

Each and every action taken by institutions of public security must be based on a transparent law, which clearly sets out their powers and duties, in line with constitutional provisions, as well as with the principle of proportionality. It is an essential democratic requirement to ensure a proper balance of rights and powers between the free citizen, on the one hand, and the public authorities, on the other. This, in turn, will also help to create more efficient internal controls within the authorities concerned. The threshold to legitimate infringements on the individual's right to privacy as well as its legal basis must be readily discernible not only to the specialists, but also for "external" observers such as top institutional management, or courts of law.

Whenever State authorities secretly process personal data of contact persons, witnesses, or third persons (especially, where these persons are eventually found innocent), the protection of their basic rights must be guaranteed by a state governed by the rule of law.

Covert observation with no clear legal basis (i.e. without a probable cause) among vaguely suspicious circles (e.g. muslims) are not acceptable in a state governed by the rule of law, and are rather reminiscent of Soviet traditions. Observation measures like of this kind are for the most part unrelated to specific criminal acts and targeted at no clear object.

In a state governed by the rule of law, there must be a probable cause based on facts to justify a specific suspicion, before any preliminary criminal investigations in the form of data processing are begun. The material facts to justify the suspicion must be documented and revealed to the data subject as soon as they no longer jeopardize the success of the investigation at hand.

At the stage of application of preliminary covert observation proceedings, an exception to the principle of transparent data processing is legitimate and justified in order to secure safety and effectiveness. Yet, to balance this out, the covert observation measures must be revealed to the data subject at a later stage, when secrecy is no longer of the essence, in order to permit for retrospective controls by the person concerned, and by the Data Supervisor. The latter must on principle have the possibility to exert controls not only retrospectively, but also prior to the measures being applied.

According to the present limitations to the competence of the EC, the Directive does not apply to the so-called "first pillar" of the EU Treaty. So far, there is no supranational law applicable to security authorities in the Member States. At the same time, there must not be a split protection of basic rights. Irrespective of EC legal regulations, it follows from Art. 116 of the *Satversme* that infringements to Art. 96 are only permissible in cases prescribed by law, i.e. on a clear and transparent normative basis.

It can thus be said that the Latvian legal provisions of material law in the area of basic laws generally meet the European standard, and are even exemplary in certain respects.

An independent and effective data protection supervision authority, as already argued more than once above, is an indispensable procedural element of the protection of protection of the basic right to privacy. The elaborates of the short-term experts have

cast further light on this problem in its relevance to the Criminal Procedure Law (see the enclosed text by Professor Paeffgen).

Finally, it should be stressed that the Data Supervisor, who will be elected by Parliament, in order to exert effective controls of the security authorities will depend on the support of specially trained staff who are well-versed in modern information technology. Procedural safeguards such as these are preconditions for a balanced upholding of personal data protection rights in the area of public security. They are moreover a requisite precondition for Latvia's readiness to join the Schengen Treaty area.

7. Concluding observations

The above observations illustrate that by putting forward constitutional amendments and legal drafts while at the same time taking into account the specifics of Latvian legal culture, the current Phare Twinning project has spurred a constitutional and legal debate that has been instrumental in winning over the Ministry of Justice's backing for certain essential amendments to the Latvian Personal Data Protection law. Provided that these amendments will be enacted accordingly, the requirements of the *acquis communautaire* would be met in an exemplary manner, also for those other Member States whose data protection legislation is yet to be brought into full compliance with the EU *acquis*. Thus, one could say – on condition that the necessary legal amendments will be adopted by Parliament – that the core objective of the present activity, as indeed of this entire Phare Twinning project will be achieved.