

FRA

Thematic Legal Study on assessment of  
data protection measures and relevant  
institutions  
in Latvia

Riga, Latvia  
February 2009

DISCLAIMER: This thematic legal study was commissioned as background material for the comparative report on *Data protection in the European Union: the role of National Data Protection Authorities* by the European Union Agency for Fundamental Rights (FRA). It was prepared under contract by the FRA's research network FRALEX. The views expressed in this thematic legal study do not necessarily reflect the views or the official position of the FRA. This study is made publicly available for information purposes only and do not constitute legal advice or legal opinion.

# Contents

<b>Executive summary .....</b>	<b>3</b>
<b>1. Overview.....</b>	<b>7</b>
<b>2. Data Protection Authority .....</b>	<b>10</b>
2.1. Legal basis .....	10
2.2. Correspondence of Powers of the DSI to Art 28 of Directive 95/46/EC 17	
2.3. Structure, budget and staffing.....	21
2.4. Independence and role of the Data State Inspectorate .....	22
<b>3. Compliance.....</b>	<b>26</b>
<b>4. Sanctions, Compensation and Legal Consequences .....</b>	<b>30</b>
<b>5. Rights Awareness.....</b>	<b>35</b>
<b>6. Analysis of deficiencies .....</b>	<b>36</b>
<b>7. Good practices .....</b>	<b>38</b>
<b>8. Miscellaneous .....</b>	<b>39</b>
<b>Annexes .....</b>	<b>40</b>

# Executive summary

## Overview

- [1]. The Constitution of Latvia provides that '[e]veryone has the right to inviolability of their private life, home and correspondence'.<sup>1</sup> Latvia has joined the main international human rights documents which protect the right to private life, including data protection, and the right to get information.<sup>2</sup> Latvia has ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,<sup>3</sup> the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow.<sup>4</sup> Latvia has started but still not finalised the ratification of the Convention on Human Rights and Biomedicine.<sup>5</sup> EU law is binding for Latvia as for any EU member state.
- [2]. The only institution directly dealing with the issue of data protection is *Datu valsts inspekcija* (DVI) [Data State Inspectorate (DSI)]. The DSI was established in 2001, half a year after the adoption of Personal data Protection Law,<sup>6</sup> in order to implement the Directive 95/46/EC. There are no NGOs working specifically in sphere of data protection.

## Data Protection Authority

- [3]. The data protection authority in Latvia is *Datu valsts inspekcija* (DVI) [Data State Inspectorate (DSI)]. The DSI is a state administration institution which is subordinated to the Ministry of Justice. The DSI started to operate in 2001, and its work was organised on the basis of

---

<sup>1</sup> Latvia/Satversme (15.02.1922), Article 96, available at [http://www.saeima.lv/LapasEnglish/Constitution\\_Visa.htm](http://www.saeima.lv/LapasEnglish/Constitution_Visa.htm).

<sup>2</sup> As the UN Declaration of Human Rights, European Convention of Human Rights; the UN International Civil and Political Rights; European Convention on Human Rights.

<sup>3</sup> Latvia/Par Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (5.04.2001), available at <http://www.dvi.gov.lv/likumdosana/g02/>.

<sup>4</sup> Latvia/Par Konvencijas par personu aizsardzību attiecībā uz personu datu automātisko apstrādi Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām (11.10.2007), available at <http://www.dvi.gov.lv/likumdosana/g03/>.

<sup>5</sup> See at [http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/webAll?SearchView&Query=\(Title=\\*biomedicinu\\*\)&SearchMax=0&SearchOrder=4](http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/webAll?SearchView&Query=(Title=*biomedicinu*)&SearchMax=0&SearchOrder=4).

<sup>6</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), available at <http://www.likumi.lv/doc.php?id=4042>

the Regulation of the Data State Inspectorate<sup>7</sup>, which sets the structure of the inspectorate, the obligations of the director of the inspectorate, as well as the financing of the inspectorate by the state budget. The Data State Inspection is headed by the director, who is appointed and released from his/her position by the Cabinet of Ministers pursuant to the recommendation of the Minister for Justice.<sup>8</sup>

- [4]. The Data State inspectorate implements the function of data protection, and is responsible for ensuring compliance with the Law on Freedom of Information.
- [5]. Although discussion on strengthening of independence of the Data State Inspectorate has been going on already for some years and a new Law on Data State Inspectorate is under elaboration, no considerable progress has yet been reached.
- [6]. The functions of the Data State Inspectorate generally correspond to requirements of the Directive 95/46/EC Article 28.

## Compliance

- [7]. Duties of registration of data processing operations and duties of requesting approval of sensitive data processing operations, as well as requirements of appointment of data protection experts are described in the Personal Data Protection Law.<sup>9</sup>
- [8]. There is not sufficient reliable information on which to evaluate how well the practice complies with data protection legislation in Latvia. Evidently, the largest data keepers are quite well aware about the legislative frame and try to comply with it. However, as the Data State Inspectorate mainly works in a reactive way, not routinely checking on data processing by its own initiative, it is still possible that there are cases where the data protection is not fully observed. There are also no NGOs in Latvia which are working specifically on data protection issues, or any other sources which could provide evidence on overall compliance.

---

<sup>7</sup> Latvia/Datu Valsts inspekcijas nolikums (28.11.2000), available at <http://www.likumi.lv/doc.php?id=13216>.

<sup>8</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 21, available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>9</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), available at <http://www.likumi.lv/doc.php?id=4042>.

## Sanctions, Compensation and Legal Consequences

- [9]. Sanctions for breaches of data protection legislation are set in the Latvian Administrative Violations Code
- [10]. The violations introduced in Latvian Administrative Violations Code are: illegal operations with a natural person's data; failure to provide information to a data subject; processing of a natural person's data without registration; failure to provide information to the Data State Inspectorate; failure to accredit persons at the Data State Inspectorate; violation of the prohibition on sending commercial information.
- [11]. The institution responsible for the examination of alleged violations of data protection foreseen by the Administrative Violations Code is the Data State Inspectorate; and its director, as well as employees authorised by him/her can take a decision and impose an administrative sanction on behalf of the Data State Inspectorate.<sup>10</sup>
- [12]. There are no known cases where compensations have been paid to persons whose data protection was not observed.
- [13]. Other legal consequences are not foreseen by laws in data protection cases.
- [14]. Enforcement of data protection legislation through sanctions payments in Latvia depends largely on the personal initiative of data subjects. Data subjects can get consultations by the Data State Inspectorate, as consulting is one of functions provided by the DSI on a regular basis. However, legal advice or legal representation is not provided by the DSI, and there are no effective NGOs in Latvia in the area of personal data protection.<sup>11</sup> Also there is no institutionalised system in Latvia for legal assistance and representation specifically in data protection cases. The financial risk of legal procedures in data protection cases is generally carried by individuals.

---

<sup>10</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (07.12.1984), Article 236<sup>10</sup>, available at <http://www.likumi.lv/doc.php?id=89648>

<sup>11</sup> Interview with Ms Aiga Balode, official of the DSI, on 3 February, 2009.

## Rights Awareness

- [15]. In addition to the Eurobarometer surveys on data protection, two more surveys on awareness of data protection have been conducted in 2005 and 2003.
- [16]. The results of the survey were interpreted as showing that awareness about data protection should be raised for state administration institutions, as well as for the public in general.

## Analysis of deficiencies

- [17]. An important deficiency regarding effective data protection and effective relevant institution is the lack of institutional independence of the Data State Inspectorate.
- [18]. As the Data State Inspectorate is responsible for the implementation and observance of all Latvian legislation concerning data protection, as well as freedom of information, both of which are complicated topics and need much awareness raising, the DSI cannot perform enough proactive work with its existent capacity. The legislative framework is worked out in order to implement the EU legislation and international standards regarding data protection, but, as the DSI has limited resources, controlling of implementation of legislation cannot be considered as sufficient.

## Good Practice

- [19]. NTR

## Miscellaneous

- [20]. NTR

# 1. Overview

- [21]. The Constitution of Latvia provides that '[e]veryone has the right to inviolability of their private life, home and correspondence'.<sup>12</sup> Latvia has joined the main international human rights documents which protect the right to private life, including data protection, and the right to get information.<sup>13</sup> Latvia has ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,<sup>14</sup> the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow.<sup>15</sup> Latvia has started but still not finalised the ratification of the Convention on Human Rights and Biomedicine.<sup>16</sup> EU law is binding for Latvia as for any EU member state.
- [22]. The national data protection legislation in Latvia is formed by a range of laws and regulations, outlined in Section 2 of the Study, and the only institution directly dealing with the issue is *Datu valsts inspekcija* (DVI) [Data State Inspectorate (DSI)]. The DSI was established in 2001, half a year after the adoption of Personal data Protection Law,<sup>17</sup> in order to implement the Directive 95/46/EC.
- [23]. The Data State Inspectorate is subordinated to the government – to the Ministry of Justice, although discussion on strengthening its independence has been going on already for some years and a new Law on Data State Inspectorate is under elaboration. However, no considerable progress has yet been reached.
- [24]. The Data State Inspectorate implements the function of data protection, and is responsible for ensuring compliance with the Law on Freedom of

---

<sup>12</sup> Latvia/Satversme (15.02.1922), Article 96, available at [http://www.saeima.lv/LapasEnglish/Constitution\\_Visa.htm](http://www.saeima.lv/LapasEnglish/Constitution_Visa.htm).

<sup>13</sup> As the UN Declaration of Human Rights, European Convention of Human Rights; the UN International Civil and Political Rights; European Convention on Human Rights.

<sup>14</sup> Latvia/Par Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (5.04.2001), available at <http://www.dvi.gov.lv/likumdosana/g02/>.

<sup>15</sup> Latvia/Par Konvencijas par personu aizsardzību attiecībā uz personu datu automātisko apstrādi Papildu protokolu par uzraudzības institūcijām un pārrobežu datu plūsmām (11.10.2007), available at <http://www.dvi.gov.lv/likumdosana/g03/>.

<sup>16</sup> See at [http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/webAll?SearchView&Query=\(Title\)=\\*biomedicinu\\*\)&SearchMax=0&SearchOrder=4](http://titania.saeima.lv/LIVS/SaeimaLIVS.nsf/webAll?SearchView&Query=(Title)=*biomedicinu*)&SearchMax=0&SearchOrder=4).

<sup>17</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), available at <http://www.likumi.lv/doc.php?id=4042>

Information. Interestingly, when adding the last function to the DSI no additional budget was foreseen.

- [25]. The Data State Inspectorate is quite active in its work, providing registration of data processing, as well as consultations and trainings on data protection. Complaints about violations of data protection are reviewed by the DSI, and administrative sanctions are imposed in case they are found to be true. The DSI actively participates in the elaboration of and by providing its opinions on legislation regarding the data protection.
- [26]. However, the capacity of the DSI is too low and the workload too big to perform proactive work and monitor the implementation of data protection legislation in practice. The DSI is not initiating court cases itself, but participates in court proceedings in cases where its decisions are appealed in court. The DSI does not defend rights of individuals in court.
- [27]. As there are no other state institutions or NGOs directly dealing with data protection issues, the work of the Data State Inspectorate is very important. However, it is difficult to assess its effectiveness. Although the DSI issues its annual reports, as is foreseen by law, these do not clearly reflect the achievements or shortcomings of the DSI. Many parts of the reports are technically copied and only slightly amended from year to year. Also, statistics are not well structured in the reports and lack meaningful subcategories, and even upon request the information provided is rudimentary at best, and thus statistical analysis and presentation appear not to be well developed in the DSI.
- [28]. The Data State Inspectorate has created quite a comprehensive web site (Latvian version), and it is also possible to obtain consultations by phone and email. This makes the data protection issue more understandable for public.
- [29]. There have not been any general public discussions on data protection in Latvia, but from time to time some specific issues have been raised in mass media on a case-by-case basis.
- [30]. It should be mentioned that some considerably important work of the Data State Inspectorate and some external lawyers working for the DVI as advisers on a contractual basis never appears in public domain, but has a crucial impact on the development of the legal frame for data protection. Such contributions are made at meetings of Parliamentary Committees in the course of preparation of legislative documents, to which experts are invited to participate. On several occasions MPs have been ready to recommend for adoption legislation which by far has not been in line with international standards on data protection. For



example, proposals have been made from different ministries to register in a unified register every case when a person visits any medical practitioner or purchases subscription medicine; or to provide the State Fire Brigade and Rescuing Service with sensitive personal data with the reasoning that it is necessary for statistics or for ensuring of better and safer work of the services. Another legislative initiative foresaw to define that data obtained during medical checkups of drivers are not sensitive personal data. These are examples of amendments to legislation which were refused after the intervention of the Data State Inspectorate and the Ombudsman Office.

## 2. Data Protection Authority

[31]. The data protection authority in Latvia is *Datu valsts inspekcija* (DVI) [Data State Inspectorate (DSI)]. The DSI is a state administration institution which is subordinated to the Ministry of Justice. The DSI started to operate in 2001, and its work was organised on the basis of the Regulation of the Data State Inspectorate<sup>18</sup>, which sets the structure of the inspectorate, the obligations of the director of the inspectorate, as well as the financing of the inspectorate by the state budget.

### 2.1. Legal basis

[32]. The initial legal basis for issuing of the Regulation of the Data State Inspectorate establishing of the Data State Inspectorate was the **Personal Data Protection Law**,<sup>19</sup> respectively, its Article 29 which defines: ‘(1) The supervision of protection of personal data shall be carried out by the Data State Inspectorate, which is subject to the supervision of the Ministry of Justice and operates independently and permanently fulfilling the functions specified in regulatory enactments, takes decisions and issues administrative acts in accordance with the law. The Data State Inspectorate is a State administration institution the functions, rights and duties of which are determined by law. The Data State Inspectorate 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 Data State Inspectorate shall act in accordance with by-laws approved by the Cabinet. Every year the Data State Inspectorate shall submit a report on its activities to the Cabinet and shall publish it in the newspaper *Latvijas Vēstnesis* [the official Gazette of the Government of Latvia].’

[33]. The Personal Data Protection Law also sets:

- duties of the Data State Inspectorate related to personal data protection: ‘1) to ensure compliance of personal data processing in the State with the requirements of this Law; 2) to take decisions and review complaints regarding the protection of personal data; 3) to register personal data processing; 4) to propose and carry out activities aimed at raising the effectiveness of personal data protection and provide

---

<sup>18</sup> Latvia/Datu Valsts inspekcijas nolikums (28.11.2000), available at <http://www.likumi.lv/doc.php?id=13216>.

<sup>19</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), available at <http://www.likumi.lv/doc.php?id=4042>.

opinions regarding the conformity of personal data processing systems to be established by the State and local governments to the requirements of regulatory enactments; 5) together with the Office of the Director General of the State Archives of Latvia, to decide on the transfer of personal data processing systems to the State archives for preservation thereof; 6) to accredit persons who wish to perform personal data processing audits in State and local government institutions. The Cabinet specifies the order how persons who wish to perform personal data processing audits in State and local government institutions shall be accredited, as well as conditions to which those persons shall comply.<sup>20</sup> In order to perform those duties, the director of the Data State Inspectorate and the Data State Inspectorate employees authorised by the director, have the right: '1) to freely enter any non-residential premises where personal data processing is located, and in the presence of a representative of the system administrator carry out necessary inspections or other measures in order to determine the compliance of the personal data processing procedure with law; 2) to require written or verbal explanations from any natural or legal person involved in personal data processing; 3) to require that documents are presented and other information is provided which relate to the personal data processing being inspected; 4) to require inspection of a personal data processing, or of any facility or information carrier of such, and to determine that an expert examination be conducted regarding questions subject to investigation; 5) to request assistance of officials of law enforcement institutions or other specialists, if required, in order to ensure performance of its duties; 6) to prepare and submit materials to law enforcement institutions in order for offenders to be held to liability, if required; to draw up a statement regarding administrative violations in personal data processing.'<sup>21</sup>

- rights of the Data State Inspectorate related to personal data protection: '1) in accordance with the procedures prescribed by regulatory enactments, to receive, free of charge, information from natural persons and legal persons as is necessary for the performance of functions pertaining to inspection; 2) to perform inspection of a personal data processing; 3) to require that data be blocked, that incorrect or unlawfully obtained data be erased or destroyed, or to order a permanent or temporary prohibition of data processing; 4) to bring an action in court for violations of this Law; 5) to cancel a personal data processing registration certificate if in inspecting the personal data processing violations are determined; 6) to impose administrative penalties according to the procedures specified by law regarding

---

<sup>20</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 29(3), available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>21</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 30(1), available at <http://www.likumi.lv/doc.php?id=4042>.

violations of personal data processing; 7) to perform inspections in order to determine the conformity of personal data processing to the requirements of regulatory enactments in cases where the system administrator has been prohibited by law to provide information to a data subject and a relevant submission has been received from the data subject.<sup>22</sup>

- [34]. The Data State Inspectorate is the national supervisory institution which performs the supervision of the national part of Schengen Information System and controls whether the rights of data subject are observed during processing of the personal data included in Schengen Information System.<sup>23</sup>
- [35]. Decisions by the Data State Inspectorate may be appealed to a court.<sup>24</sup>
- [36]. The **Electronic Documents Law** sets functions of the State Data Inspectorate: in regard to supervision of trusted certification service providers: ‘The State Data Inspectorate shall be the supervisory institution for trusted certification service providers. The supervisory institution shall regularly supervise the conformity of the work of the trusted certification service providers to the requirements of this Law and other regulatory enactments.’<sup>25</sup>
- [37]. The Electronic Documents Law foresees:
- duties of the State Data Inspectorate: ‘1) to accredit certification service providers in accordance with the voluntary accreditation principles; 2) to check whether the trusted certification service providers comply with the certification service provision regulations; 3) to monitor that the security of the trusted certification service provider information system and procedures conform to this Law, other regulatory enactments and the description of the trusted certification service provider information system, equipment and procedure security; 4) to monitor that the electronic signature-verification data and time-stamp registers for qualified certificates issued, revoked, suspended and renewed by trusted certification service providers is accessible in an on-line regime; 5) to ensure that the Latvian accredited trusted certification service provider register in which information regarding certification service providers from other states is also included, the issued qualified certificates of

---

<sup>22</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 29(4), available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>23</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 30<sup>1</sup>, available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>24</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 31, available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>25</sup> Latvia/Elektronisko dokumentu likums (31.10.2002), Article 19, available at <http://www.likumi.lv/doc.php?id=68521>.

which are guaranteed by a Republic of Latvia accredited trusted certification service provider, is freely accessible in an on-line regime'.<sup>26</sup> The supervisory institution for trusted certification service providers shall 'maintain an on-line freely accessible trusted certification service provider register. If the documents submitted and the certification service provider conform to the requirements of this Law and other regulatory enactments, the supervisory institution shall issue, within a period of 10 days from receipt of all the documents referred to in Section 10 of this Law, to the certification service provider an accreditation certificate and shall include the information referred to in Paragraph two of this Section in the trusted certification service provider register. If the documents submitted or the certification service provider do not conform to the requirements of this Law and other regulatory enactments, the supervisory institution shall issue, within a period of 10 days from receipt of all the documents referred to in Section 10 of this Law, a written refusal of accreditation.'<sup>27</sup>

- supervisory measures which can be implemented by the State Data Inspectorate: (1) The supervisory institution has the right to give instructions to trusted certification service providers to rectify non-conformity with this Law, other regulatory enactments, the certification service provision regulations included in the trusted certification service provider register or the description of the certification service provision information system, equipment and procedure security; (2) The time period for rectification of non-conformity shall be determined by the supervisory institution; (3) If the supervisory institution's instructions are not carried out within the time period specified by it, the supervisory institution shall warn the trusted certification service provider regarding the possible revocation of accreditation; (4) If, within 10 days following the supervisory institution's warning regarding the possible revocation of accreditation, the supervisory institution's instructions are not carried out, the accreditation of the trusted certification service provider shall be revoked without delay and the information regarding the revocation of the accreditation shall be included in the trusted certification service provider register. In performing supervision, officials of the supervisory institution shall present a service identification document. The person referred to has the following rights:  
1) to freely visit any commercial premises in which the information systems and equipment of the trusted certification service provider is located, and in the presence of the certification service provider to perform the necessary examination or other measures, in order to

---

<sup>26</sup> Latvia/Elektronisko dokumentu likums (31.10.2002), Article 20(1), available at <http://www.likumi.lv/doc.php?id=68521>.

<sup>27</sup> Latvia/Elektronisko dokumentu likums (31.10.2002), Article 20(2)(3)(4), available at <http://www.likumi.lv/doc.php?id=68521>.

determine the conformity of the certification service provision process to this Law, other regulatory enactments, certification service provision regulations published in the trusted certification service providers register and the description of the certification service provision information system, equipment and procedure security; 2) to request written or oral explanations from the trusted certification service provider representatives and employees; 3) to become acquainted with documents and other information which relate to certification service provision; and 4) to request the examination of the information systems, equipment and procedures of the trusted certification service provider and to specify the issues to be investigated in the independent expert-examination.

(7) The supervisory institution has the right to bring an action in court to terminate the activities of a trusted certification service provider if the relevant trusted certification service provider violates this Law or other regulatory enactments.<sup>28</sup>

- [38]. The decisions of the supervisory institution for trusted certification service providers – the Data State Inspectorate – may be appealed to a court.<sup>29</sup>
- [39]. The Data State Inspectorate also supervises the observance of the **Freedom of Information Law** which ensures public access to information which is under the control of State administrative institutions and Local Government institutions for the performance of their specified functions as prescribed in regulatory enactments. The Freedom of Information Law determines a uniform procedure by which natural and legal persons are entitled to obtain information from State administrative institutions and Local Government institutions, and to utilise it.<sup>30</sup>
- [40]. According to the **Electronic Communications Law**, the protection of personal data in the electronic communications sector also shall be supervised by the State Data Inspection. In order to ensure the referred to supervision, the State Data Inspection has the rights specified in the **Personal Data Protection Law** (see above).<sup>31</sup>

---

<sup>28</sup> Latvia/Elektronisko dokumentu likums (31.10.2002), Article 21, available at <http://www.dvi.gov.lv/eng/legislation/edl/>.

<sup>29</sup> Latvia/Elektronisko dokumentu likums (31.10.2002), Article 21(8), available at <http://www.dvi.gov.lv/eng/legislation/edl/>.

<sup>30</sup> Latvia/Informācijas atklāfības likums (29.10.1998), Article 2, Article 19, available at <http://www.likumi.lv/doc.php?id=50601>.

<sup>31</sup> Latvia/Elektronisko sakaru likums (28.10.2004), Article 4(4), available at <http://www.likumi.lv/doc.php?id=96611>.

- [41]. The **Law on Information Society Services** provide the Data State Inspectorate with power to supervise within its competence the circulation of information society services,<sup>32</sup> and sets the obligation to provide service providers and service recipients with information regarding the procedures for the examination of complaints and other information.<sup>33</sup>
- [42]. Under the Law on Information Society Services the Data State Inspectorate has the following rights and duties: 1) ‘if a supervisory body detects violations of this Law, it is entitled to request all the information necessary for the clarification of the substance of a case and order the service provider to stop the violation of the Law or to perform particular activities for the elimination thereof, as well as to specify the time period for the execution of these activities; 2) a supervisory body is entitled to perform the [aforementioned] activities, which restrict the provision of such an information society service which creates or may create serious risk if these activities are proportional to the protection of the relevant interests and are necessary for the interests of the public, especially for the prevention and investigation of criminal offences and the initiation of criminal offence proceedings, including the protection of minors in order to prevent the discrimination of a person due to his or her race, gender, religious convictions or ethnic origin, as well as violations injuring the dignity and honour of a person; for public safety, including national security and defence; for public health protection; for consumer protection; 3) prior to performing [those restrictive] activities, a supervisory body shall inform the State supervisory body in which the relevant service provider is registered and request that it take actions in order to stop the violation [...]. The supervisory body of Latvia shall inform the European Commission and the relevant state regarding activities they are planning to perform if that state do not perform activities for the elimination of the violation or the activities performed thereby are not sufficient; 4) in urgent cases when there is a justified reason to deem that public safety, health or consumer interests are endangered, a supervisory body may perform the [aforementioned] activities prior to informing the European Commission and the relevant state. In such case, the supervisory body shall immediately inform the European Commission and the relevant

---

<sup>32</sup> Information society service - a distance service (parties do not meet simultaneously) which is usually a paid service provided using electronic means (electronic information processing and storage equipment, including digit compression equipment) and upon the individual request of a recipient of the service. Information society services include the electronic trade of goods and services, the sending of commercial communications, the possibilities offered for searching for information, access to this and the obtaining of information, services that ensure the transmission of information in an electronic communication network or access to an electronic communication network, and storage of information

<sup>33</sup> Latvia/Informācijas sabiedrības pakalpojumu likums (4.11.2004), Article 12 available at <http://www.likumi.lv/doc.php?id=96619>.

state regarding the performed activities and justify the urgency of these activities.<sup>34</sup>

- [43]. **The Law on System of Processing of Biometric Data** stipulates that the Data State Inspectorate shall supervise the observance of that law in accordance with laws regulating personal data protection.<sup>35</sup>
- [44]. **The Human Genome Research Law** provides that ‘the State Data Inspection shall perform the supervision of the collection of the descriptions of the state of health and genealogical data, coding and decoding of tissue samples, descriptions of DNA, descriptions of the state of health and genealogical data, as well as processing of tissue samples, descriptions of DNA, descriptions of the state of health and genealogical data.’<sup>36</sup>
- [45]. The **Latvia’s Administrative Violations Code** grants the Data State Inspectorate an obligation to ‘examine the administrative violation matters provided for in Sections 204.<sup>7</sup> [Illegal Operations with a Natural Person’s Data], 204.<sup>8</sup> [Failure to Provide Information to a Data Subject], 204.<sup>9</sup> [Processing of a Natural Person’s Data without Registration], 204.<sup>10</sup> [Failure to Provide Information to the Data State Inspectorate], 204.<sup>11</sup> [Failure to Accredit Persons at the Data State Inspectorate] and 204.<sup>16</sup> [Violation of the Prohibition on Sending Commercial Information] of this Code. The Data State Inspectorate Director and his/her authorised employees are entitled to examine administrative violation matters and to impose an administrative sanction on behalf of the Data State Inspectorate.’<sup>37</sup>
- [46]. The decisions of the Data State Inspectorate can be appealed to the Administrative Court by general order, set by **the Administrative Procedure Law**.<sup>38</sup>

---

<sup>34</sup> Latvia/Informācijas sabiedrības pakalpojumu likums (4.11.2004), Article 12, available at <http://www.likumi.lv/doc.php?id=96619>.

<sup>35</sup> Latvia/Biometrijas datu apstrādes sistēmas likums (31.05.2007), Article 16, available at <http://www.likumi.lv/doc.php?id=158772>.

<sup>36</sup> Latvia/Cilvēka genoma izpētes likums (13.06.2002), Article 21, available at <http://www.likumi.lv/doc.php?mode=DOC&id=64093>.

<sup>37</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (7.12.1984), Article 236.<sup>10</sup>, available at <http://www.likumi.lv/doc.php?id=89648>.

<sup>38</sup> Latvia/ Administratīvā procesa liums (25.10.2001), available at <http://www.likumi.lv/doc.php?id=55567>.



## 2.2. Correspondence of Powers of the DSI to Art 28 of Directive 95/46/EC

- [47]. Directive 95/46/EC Article 28, paragraph 2.<sup>39</sup> Although the duty to consult the authorities in the process of drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data is not explicitly set in the laws regulating the work of the Data State Inspectorate, that institution has actively participated in the elaboration of legislation and policy documents at different levels already since the very beginning of its work. For example, in the first year (2001) the DSI drafted amendments to the Personal Data Protection Law, the Administrative Violations Code, the Law on Police, the Law on Taxes and Duties, and in the Cabinet Regulation No. 226 'List of Units of the State Secret'.<sup>40</sup> The Director of the Data State Inspectorate led a governmental working group for the elaboration of amendments to the Administrative Violations Code – a new chapter on liability for breaches related to information technologies. The officials of the DSI also participated in governmental working groups on drafts of the Electronic Documents Law, the Conception and Action Plan for Electronic Commerce, the Conception of E-governance, as well as on data protection issues regarding the Schengen Agreement. In 2007, the DSI elaborated 13 drafts of laws and regulations and provided 18 opinions with regard to drafts of legislation and policy documents related to the data protection issues. Many of those opinions concerned international treaties and international legislation. The DSI also elaborated in 2007 a policy document 'Strategy of work of the Data State Inspectorate 2007-2009', defining its main goals and tasks, as well as identifying problematic issues. Evidently, work on legislation issues is a substantial part of the work of the Data State Inspectorate.
- [48]. Directive 95/46/EC Article 28, paragraph 3.<sup>41</sup> The powers corresponding to those required to be granted to data protection

---

<sup>39</sup> 'Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data'.

<sup>40</sup> Pārskats 2001

<sup>41</sup> 'Each authority shall in particular be endowed with: investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties; effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions; the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these

authority by the paragraph 3 of Article 28 of the Directive 95/46/EC are settled to the Data State Inspectorate by laws which regulate its work and set the functions, duties and rights of the DSI. (See Chapter 2.1. ‘Legal basis and powers’.) The decisions of the Data State Inspectorate can be appealed to the Administrative court under the Administrative Procedure Law within a month from when they become effective.

- [49]. Notwithstanding positive practice, consultation with DSI on administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regards to the processing of personal data is discretionary, as it is not set in any law or regulation. The DSI does, however, according to the Personal Data Protection Law have the duty to initiate measures to improve personal data protection, as well as to provide opinions on state and municipal authorities’ formed personal data processing systems’ compliance with normative enactments (Article 29. (3) 4)).
- [50]. In the field of personal data protection, the DSI has, according to Article 29 (4) of the Personal Data Protection Law, general investigative rights, such as the right to obtain all necessary information for the performance of the duties of the DSI from physical and legal persons free of charge and the right to conduct inspections of personal data processing. In addition, in order to perform the DSI set duties, the DSI director or staff member with the director’s power of attorney has the investigative rights set in Article 30 (1), such as freely access any relevant non-residential premises where data processing is located and perform inspections or take other measures, in the presence of the controller, in order to verify the compliance with the law of any data processing procedures, to request written or oral explanation from any physical or legal person connected with data processing, to request to be shown documents and be provided with other information relating to the inspected personal data processing, to request the control of personal data processing and any related equipment or information carrier and to order an expert analysis for the examination of the issue under inspection. However, the duty of the physical or legal person who is requested such information by DSI to reply is not specified in this law, although the Administrative Violations Code includes the violation of not providing information to DSI.
- [51]. The DSI powers of intervention include the rights to request the blocking of data, the erasure or destruction of incorrect or illegally obtained data, to prohibit temporarily or permanently the processing of data. In addition, the DSI has powers to annul personal data processing registration licenses if during inspection of personal data processing

---

violations to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.’

violations are found and the powers to impose administrative violations fines for violations of personal data processing (Article 29(4), and the DSI director or authorised person also has the right to file a protocol on administrative offense with regards to personal data processing (Article 30 (1) 7)).

- [52]. The Administrative Violations' Code provides the DSI with the right to impose a fine or to issue a warning for specific violations (See Chapter 4.). Nevertheless, issuing of warnings or admonishing a controller are not listed among the powers of DSI or its director in the Personal Data Protection Law, nor are powers to refer the case to the national parliament or other political institutions. Also, although the duty to adopt decisions relating to personal data protection is set in the Personal Data Protection Law Article 29 (3) 2), the corresponding powers have not been listed among the DSI rights in either Article 29 or Article 30 of the same law.
- [53]. In terms of powers to engage in legal proceedings, the DSI has the power to submit an application to court on violations of the Personal Data Protection Law (Article 29 (4) 4)). The DSI director or a person authorised by the director also has the powers, in order to ensure the performance of the DSI duties, to prepare and submit materials to law enforcement institutions in order to call a guilty person to criminal responsibility (Article 30 (1) 6)).
- [54]. Directive 95/46/EC Article 28, paragraph 4.<sup>42</sup> The Data State Inspectorate has an explicitly set duty to make decisions and review complaints regarding the protection of personal data.<sup>43</sup> Persons concerned shall be informed of the outcome of claims in the order established by the Administrative Procedure Law<sup>44</sup> and the Law on Submissions.<sup>45</sup> In line with rising public awareness about data protection issues, the number of complaints received by the DSI is growing. There were 38 complaints submitted to the DSI in 2001 (11 found to be well-founded), 86 in 2002, and 120 in 2007 (approximately 30 were well-founded, and in 20 out of those cases administrative

---

<sup>42</sup> 'Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim. Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.'

<sup>43</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), available at <http://www.likumi.lv/doc.php?id=4042> .

<sup>44</sup> Latvia/ Administratīvā procesa likums (25.10.2001), available at <http://www.likumi.lv/doc.php?id=55567> .

<sup>45</sup> Latvia/Iesniegumu likums (27.09.2007), available at <http://www.likumi.lv/doc.php?id=164501> .

penalties were imposed by the DSI).<sup>46</sup> Most frequent complaints concerned the processing of personal data without any legitimate aim, as well as exceeding the amount necessary for achieving of a legitimate goal. Concerns about possible breaches regarding personal data processing were most often raised in relation to return of credits and the development of credit history, data processing performed by in-house-managers, video-surveillance and copying of passports.<sup>47</sup>

- [55]. Additional powers needed by the DSI in order to ensure effective personal data protection include the right to consult the authorities on any proposals for normative or regulatory acts relating to personal data protection. For investigative powers, in addition to the right to request information from physical and physical persons, the law should also set the right of the DSI to receive an answer to such questions. The right to impose administrative fines would be more effective in ensuring compliance with request by the DSI if the powers were not limited only to the substance of personal data protection, but also would include, within the limits of the law, the procedural aspects of DSI work, such as access to premises and information.
- [56]. The DSI remit is broad and covers personal data protection of natural persons, public access to information of state and municipal administrative institutions and supervision of trusted certification service providers.
- [57]. The Personal Data Protection Law covers all natural persons' fundamental rights and freedoms in relation to the processing of personal data. The law applies to all natural and legal persons if the controller is registered in the Republic of Latvia, the data processing takes place outside the borders of the Republic of Latvia, but on territory which belongs to the Republic of Latvia in accordance with international agreements, if the equipment, which is used to process the data is located on the territory of Latvia, except where such equipment is used solely for transferring personal data through the territory of the Republic of Latvia. The law does not apply to personal data processing performed by natural persons for purposes of domestic or family needs and the personal data is not disclosed to third parties. (Article 3).

---

<sup>46</sup> DVI pārskati

<sup>47</sup> DVI pārskats 2007

## 2.3. Structure, budget and staffing

- [58]. The Data State Inspection Sample is headed by the director, who is appointed and released from his/her position by the Cabinet of Ministers pursuant to the recommendation of the Minister for Justice.<sup>48</sup>
- [59]. The structure and organisation of the Data State Inspectorate, as well as the competences of its employees and departments are set by the Regulation on the Data State Inspectorate, issued on basis of Article 75(1) of the State Administration Structure Law<sup>49, 50</sup>.
- [60]. The Regulation on the Data State Inspectorate stipulates that Data State Inspectorate is managed by a director who has two deputies: a Deputy Director on Strategy and General Issues and Deputy Director on Control Issues.
- [61]. The Data State Inspectorate is divided into permanent divisions: Administrative Division, Legal Division, Development Division, Security Division, Supervision Division, Registration Division, and 3<sup>rd</sup> Pillar Data Supervision Division.
- [62]. The number of employees of the Data State Inspectorate has more than doubled since its establishment in 2001,<sup>51</sup> and for the last two years there have been 23 employees, which corresponds to 78 per cent of necessary staffing. However, in 2008, in line with restrictive economic measures related to the state administration overall, 5 employees were fired, thus considerably complicating the execution of the functions of the Inspectorate.
- [63]. The budget of the Data State Inspectorate since its creation has grown considerably: from Ls 100,182.00 (approximately 142,546.00 EUR) in 2001 to Ls 518,771.00 (738,145.00 EUR) in 2007. At the same time, the number of functions set for the DSI has grown during those years. For example, although since 2004 the DSI is responsible for supervision of observance of the Freedom of Information Law, budgetary means for implementation of this function have not been allocated.<sup>52</sup>

---

<sup>48</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 21, available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>49</sup> 'The regulations of an institution of direct administration shall be issued by the head of such institution. The draft regulations shall be co-ordinated with a higher institution or a member of the Cabinet if the institution is directly subordinate to such member.'

<sup>50</sup> Latvia/Datu valsts inspekcijas reglaments (12.10.2007), available at [http://www.dvi.gov.lv/par\\_mums/files/DVI\\_reglaments.pdf](http://www.dvi.gov.lv/par_mums/files/DVI_reglaments.pdf).

<sup>51</sup> See the Annex 1.

<sup>52</sup> Information provided by Ms Aiga Balode, the official of the Data State Inspectorate, on 13 February, 2009.

- [64]. In 2004, 2005 and 2006 a significant part of the budget was formed by means from PHARE project Nr. 2002/00-590-03-01 „Data State Inspectorate”.<sup>53</sup> However, the budget allocated for 2009 – again because of over-all budget cut-backs – will be at the level of 2003: approximately Ls 370,000.00 (526,462.00 EUR).<sup>54</sup> Obviously, that, as well as reduction of number of employees, will not be of help for increasing the effectiveness of the work of the Data State Inspectorate.

## 2.4. Independence and role of the Data State Inspectorate

- [65]. Although the Personal Data Protection Law sets that the Data State Inspectorate operates independently, in the same sentence it denotes that the DSI is subject to the supervision of the Ministry of Justice.<sup>55</sup> Such status of a subordinated institution, which is not structurally independent from political power potentially undermines both the independence and effectiveness of the institution, for example with regard to financing, to implementation of controlling function over supervisory body, etc.
- [66]. The concern over insufficient independence, which does not conform to requirement by the Directive 95/46/EC, was raised already some years ago. One of the main goals of the PHARE project ‘The Data state Inspectorate’, which was implemented from 15 September 2004 to 15 September 2005, was to elaborate amendments to legislation, providing the DSI with full independence. On 18 May 2005 the Cabinet approved the Concept of the Status of Independent Institutions where the necessity to change the status of the DSI, which is subordinated to the political power, was explicitly set. On 3 November 2006 the Cabinet also approved the Action Plan 2007-2009 for the Ministry of Justice<sup>56</sup> which foresaw to transform the DSI to an independent institution in 2007. The necessity to strengthen the independence of the DSI was indicated also in conclusions of the Schengen evaluation. In 2006 a draft Law on the Data State Inspectorate was elaborated by the Data State Inspectorate, in order to set the legal status, functions and tasks of

---

<sup>53</sup> In 2004 financing provided for the DSI by the State was Ls 382,748.00 (544,601.00 EUR), by PHARE program – Ls 218,314.00 (310,633.00 EUR); in 2005 respectively Ls 286,704.00 (407,943.00 EUR) and Ls 293,070.00 (417,001.00 EUR); in 2006 – Ls 305,349.00 (434,472.00 EUR) and Ls 66,759.00 (94,989.00 EUR).

<sup>54</sup> Information provided by Ms Aiga Balode, the official of the Data State Inspectorate, on 30 January, 2009.

<sup>55</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 29, available at <http://www.likumi.lv/doc.php?id=4042>

<sup>56</sup> Latvia/Aktualizētā Tieslietu ministrijas darbības stratēģija 2007.-2009. gadam (7.11.2007), available at <http://polsis.mk.gov.lv/LoadAtt/file46199.doc>.

the DSI, as well as the order by which the DSI realizes its functions and tasks set by the law to protect the rights of individuals with regard to personal data, as well as to promote access for individuals to information from state and municipal institutions.<sup>57</sup> The final elaboration of the draft law and the passing of it in Parliament were set as the main tasks for 2008.<sup>58</sup> However, in 2009 there has not been any considerable progress, and the law is still under elaboration.

[67]. With the functions the laws provide to the Data State Inspectorate at the moment, it has a power to become active on its own initiative. However, as it appears in the annual reports of the DSI, as well as in interviews with the officials of the DSI, the work of data protection institution in Latvia is mainly reactive, not proactive. It could be explained by the amount of functions the DSI has to carry out and the insufficient resources available for performance of those functions. The only recent case where the DSI has made an inspection on its own initiative, which was described in the annual report and also mentioned by the official of the DSI during the interview, was related to checking of seven hotels in Riga (from 20 July to 15 August 2007), reviewing the overall order of processing of personal data of hotels guests, as well as the level of awareness among staff of the hotels about issues of data protection. In particular, the processing of personal data for purposes of use of electronic cards and magnetic cards which store personal information was checked, as well as the processing of personal data obtained during video-surveillance. The DSI found that in general hotels are processing data accordingly to requirements of the Personal Data Protection Law. However, the DSI found that several hotels have not registered personal data processing as it is set by the Personal Data Protection Law. Some hotels were making copies of passports of guests, thus collecting data in excess of the amount of data processing necessary for achieving of the aim. In some cases personal data were stored longer than necessary for achieving of the aim of their processing, thus breaching the Personal Data Protection Law, Article 10(1.3). After the inspection the DSI sent letters to the hotels indicating their main duties in respect to personal data protection, shortcomings which were found during the inspection, as well as recommendations how to prevent them.<sup>59</sup>

[68]. Interviews with officials of the Data State Inspectorate indicated that the monitoring role of the DSI is implemented quite poorly, limiting it to sporadic monitoring of information in mass media, as well as so-

---

<sup>57</sup> 2006. gada pārskats, available at [http://www.dvi.gov.lv/par\\_mums/files/Gada\\_parskats\\_2006\\_DVI.pdf](http://www.dvi.gov.lv/par_mums/files/Gada_parskats_2006_DVI.pdf).

<sup>58</sup> 2007. gada pārskats

<sup>59</sup> 2007. gada pārskats,

called follow-up monitoring regarding implementation of decisions of the DSI.<sup>60</sup>

- [69]. Decisions and opinions of the Data State Inspectorate are not readily available to the public. Although the DSI has a web site with quite extensive information regarding data protection and the DSI itself, opinions and some decisions are only briefly summarised in annual reports of the DSI. As the decisions and opinions of the DSI in general are not classified information, it is possible to request them from the DSI. However, particularly in regard to cases related to personal data, the DSI makes the argument that making decisions publicly available will breach individual's right to personal data protection, but the removal of actual names from the decisions, which could prevent this, is a time-consuming process, requiring resources of the DSI.<sup>61</sup>
- [70]. The Opinions of the Working Party established under Article 29 of Directive 95/46/EC are considered by the Data State Inspectorate as recommendations how to interpret national legislation implementing the EU legislation on data protection, and references are made in the opinions of the DSI to those Opinions. The latest Opinions are put on web site of the DSI (summary and full text).<sup>62</sup>
- [71]. The advisory function of the DSI, both at the legislative level and the level of data subject/data processor, is one of the most important areas of its work. The DSI provides consultations on data protection issues by phone every day from 2 p.m. to 4 p.m., as well as personal consultations by appointment.<sup>63</sup> Advisory activities regarding the legislation are described in paragraph [40] of the report.
- [72]. The Data State Inspectorate attaches great importance to the implementation of its awareness raising function. Particularly during the first years of work of the DSI that was considered as a very important goal – to inform society on data protection issues, as there was low awareness of that notion. Since then the DVI still keeps awareness raising as one of top priorities of its work. In 2002, the DSI web site ([www.dsi.gov.lv](http://www.dsi.gov.lv)) in Latvian, Russian and English was developed, containing regularly updated information (however, mainly only in the Latvian version) on actual issues regarding data protection, legislation, international standards and documents regarding the data protection, etc. In 2007 the web site has been visited 2000-6000 times a month. Also, an information e-mail address ([info@dvi.gov.lv](mailto:info@dvi.gov.lv)) was

---

<sup>60</sup> Information provided by Ms Aiga Balode, the official of the Data State Inspectorate, on 13 February, 2009.

<sup>61</sup> Information provided by Ms Aiga Balode, the official of the Data State Inspectorate, on 16 February, 2009 .

<sup>62</sup> See at <http://www.dvi.gov.lv/jaunumi/> .

<sup>63</sup> See at <http://www.dvi.gov.lv/jaunumi/read.php?c=&id=1232471703.180.1.1> .



created in order to give an opportunity to efficiently contact the DSI and to request information electronically. The DSI has established cooperation with mass media, using media venues for informing the public about data protection issues. The DSI has provided seminars for particular target groups in order to inform on their duties and rights regarding to data protection. For example, in 2007 seminars were delivered to school directors and teachers, IT specialists, internal auditors. Informational seminars were delivered also on amendments to the Personal Data Protection Law. The DSI also has issued several publications. Thus, in 2006 a bulletin on Personal Data Protection was issued;<sup>64</sup> in 2007 bulletin on Personal Data in Schengen Information System was published and distributed, and informative material on Registration of Personal Data Processing was prepared. In 2007 an educational competition 'Don't Let Anybody Else Take Your Place' was launched among teenagers, bearing in mind that the Working Party established under Article 29 of Directive 95/46/EC had set teenagers as priority target group for 2007.

---

<sup>64</sup> Available at [http://www.dvi.gov.lv/files/1.1\\_Brosura\\_tiesl\\_min\\_A5.pdf](http://www.dvi.gov.lv/files/1.1_Brosura_tiesl_min_A5.pdf) .

### 3. Compliance

- [73]. Personal data processing is permitted only if law does not prescribe otherwise, 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, taking into account a request from the data subject, the processing of data is necessary in order to enter into the relevant contract; 3) the data processing is necessary to an administrator for the performance of his or her duties as specified by law; 4) the data processing is necessary to protect vitally important interests of the data subject, including life and health; 5) the 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 an administrator or transmitted to a third person; and 6) the 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 administrator or of such third person as the personal data have been disclosed to.<sup>65</sup>
- [74]. In order to protect the interests of a data subject, an administrator shall ensure that: 1) the personal data processing takes place with integrity and lawfully; 2) the personal data is processed only in conformity with the intended purpose and to the extent required therefor; 3) the personal data are stored so that the data subject is identifiable during a relevant period of time, which does not exceed the time period prescribed for the intended purpose of the data processing; and 4) the personal data are accurate and that they are updated, rectified or erased in a timely manner if such personal data are incomplete or inaccurate in accordance with the purpose of the personal data processing. Personal data processing for purposes other than those originally intended is permissible if it does not violate the rights of the data subject and is carried out for the needs of scientific or statistical research only in accordance with the conditions referred to in the Personal Data Protection Law.<sup>66</sup>
- [75]. The processing of sensitive personal data is prohibited, except in cases where: 1) the data subject has given his or her written consent for the processing of his or her sensitive personal data; 2) special processing of

---

<sup>65</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 7, available at <http://www.likumi.lv/doc.php?id=4042>.

<sup>66</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 10, available at <http://www.likumi.lv/doc.php?id=4042>.

personal data, without requesting the consent of the data subject, is provided for by regulatory enactments, which regulate legal relations regarding employment, and such regulatory enactments guarantee the protection of personal data; 3) personal data processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent; 4) personal data processing is necessary to achieve the lawful, non-commercial objectives of public organisations and their associations, if such data processing is only related to the members of these organisations or their associations and the personal data are not transferred to third parties; 5) personal data processing is necessary for the purposes of medical treatment, the provision of health care services or the administration thereof and the distribution of medication and medical equipment or their administration; 6) the processing concerns such personal data as necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings; 7) personal data processing is necessary for the provision of social assistance and it is performed by the provider of social assistance services; 8) personal data processing is necessary for the establishment of Latvian national archive holdings and it is performed by the State archives and institutions with State storage rights approved by the Director-general of the State archives; 9) personal data processing is necessary for statistical research, which is performed by the Central Statistics Bureau; and 10) the processing relates to such personal data, which the data subject has him or herself made public; 11) personal data processing is necessary for execution of state administration functions or for developing of state information systems which are foreseen by the law.<sup>67</sup> If personal data, which relate to the commitment of criminal offences, convictions in criminal matters, court proceedings in criminal matters and closed court sittings in civil matters, only persons authorised by law are entitled to process such data and in the cases specified by law.<sup>68</sup>

- [76]. All State and local government institutions, and other natural persons and legal persons which carry out or wish to commence carrying out personal data processing, shall register such in accordance with the procedures prescribed in the Personal Data Protection Law. The registration procedure prescribed by that Law is not applicable to 1) personal data processing for the needs of accounting and personnel registration; 2) State or local government information systems where collected personal data are publicly available; 3) journalistic needs in

---

<sup>67</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 11, available at <http://www.likumi.lv/doc.php?id=4042> .

<sup>68</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 12, available at <http://www.likumi.lv/doc.php?id=4042> .

accordance to the Law 'On Press and Other Mass Media'; 4) archive needs in accordance to Law 'On Archives'; 5) personal data processing managed by religious organisations; 6) cases where administrator has registered a personal data protection expert.<sup>69</sup>

- [77]. Administrator is allowed not to register personal data processing if he/her appoints a personal data protection expert. A personal data protection expert is not a personal data processor. A person can be appointed as personal data protection expert if he/she has an university degree in law, IT or similar area and has been instructed in accordance to order set by the Cabinet. The administrator shall provide the personal data protection expert with necessary means, information, and schedules time for performance of personal data protection expert duties within working hours. The administrator shall register the personal data protection expert in the Data state Inspectorate. If the personal data protection expert performs audit of personal data processing he/she has not to be registered in the Data State Inspectorate additionally. The register of personal data protection experts is publicly available and contains following information about personal data protection expert: 1) name, family name, contacts; 2) term of appointment; 3) place of personal data processing and data about possibility to get information which shall be provided to the DSI in case of data processing.<sup>70</sup>
- [78]. The institutions and persons referred in the Personal Data Protection Law which wish to commence personal data processing shall submit an application for registration to the Data State Inspectorate which includes the following information: 1) name, family name and personal code (name and registration number for legal entities), address and phone of the administrator; 2) name, family name and personal code, address and phone of the personal data processor (if there is such); 3) legal ground for personal data processing; 4) kinds of personal data and aims for processing of personal data; 5) categories of data subjects; 6) categories of recipients of personal data; 7) intended method of personal data processing; 8) planned method of obtaining of personal data; 9) place of processing of personal data; 10) holder of information resources or technical resources, as well as person who is responsible for security of information system; 11) technical and organisational activities performed in order to ensure personal data protection; 12) which personal data will be transferred to other states which are not EU member states or member states of the European Economic Zone. The Data State Inspectorate shall identify the personal data processing

---

<sup>69</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 21, available at <http://www.likumi.lv/doc.php?id=4042> .

<sup>70</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 21<sup>1</sup>, available at <http://www.likumi.lv/doc.php?id=4042> .

which can create a risk to rights and freedoms of data subjects. A prior checking must be performed for processing of those personal data. When registering a personal data processing, the Data State Inspectorate shall issue a certificate of registration of the personal data processing to an administrator or authorised person.<sup>71</sup>

- [79]. Persons involved in personal data processing shall make a commitment in writing to preserve and not, in an unlawful manner, disclose personal data. Such persons have a duty not to disclose the personal data even after termination of employment or other contractually specified relations. An administrator is obliged to maintain a record of those persons.<sup>72</sup>
- [80]. As the system of registration was changed by amendments of 1.03.2007 to the Personal Data Protection Law (in force since 1.09.2007) in order to make data processing easier and speed it up, the Data State Inspectorate has provided more than 500 consultations to administrators on this matter in period from 1 September 2007 to 31 December 2007. 182 personal data processing were registered in that period.
- [81]. There is no reliable ground to evaluate how well the practice complies with data protection legislation in Latvia. Evidently, the largest data keepers are quite well aware about the legislative frame and try to comply with it, however, as the Data State Inspectorate mainly works in a reactive way, not routinely checking on data processing by its own initiative, it is still possible that there are cases where the data protection is not fully observed. There are also no NGOs in Latvia which are working specifically on data protection issues, or any other sources which could provide evidence on overall compliance.

---

<sup>71</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 22, available at <http://www.likumi.lv/doc.php?id=4042> .

<sup>72</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 27, available at <http://www.likumi.lv/doc.php?id=4042> .

## 4. Sanctions, Compensation and Legal Consequences

[82]. Sanctions for breaches of data protection legislation are set in the Latvian Administrative Violations Code, which stipulates that ‘an administrative violation shall be acknowledged as an unlawful, blameable (committed with intent or through negligence) action or inaction, which endangers State or public order, property, rights and freedoms of citizens or management procedures specified and regarding which administrative liability is specified in the Law.’<sup>73</sup> Further, the explanation of the notions of ‘Commitment of an Administrative Violation with Intent’ and ‘Commitment of an Administrative Violation Through Negligence’ are provided by the law,<sup>74</sup> and it is stated that ‘in imposing a sanction [...], the degree of violator’s culpability [...] shall be taken into account.’<sup>75</sup> It follows from this that proof of intent or negligence can be taken into account in imposing administrative sanctions for breach of data protection laws.

[83]. The violations introduced in Latvian Administrative Violations Code are:

- **Illegal Operations with a Natural Person’s Data.**

‘In the case of the illegal operations with a natural person’s data, that is, in respect of any illegal operations with a natural person’s data, including collection of data, registration entering, storing, ordering, transforming, utilisation, transfer, transmitting, blocking or deleting, a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 50 [71 EUR] up to LVL 400 [570 EUR], on officials – from LVL 100 [142 EUR] up to LVL 400 [570 EUR], but for legal persons – from LVL 1000 [1423 EUR] up to LVL 8000 [11,383 EUR], with or without confiscation of the articles and tools used to commit the violation.

In the case of the illegal operations with a natural person’s sensitive personal data, that is, in respect of any illegal operations with a natural person’s sensitive personal data, including collection of data, registration entering, storing, ordering, transforming, utilisation,

---

<sup>73</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (07.12.1984), Article 9, available at <http://www.likumi.lv/doc.php?id=89648>.

<sup>74</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (07.12.1984), Article 10, Article 11, available at <http://www.likumi.lv/doc.php?id=89648>.

<sup>75</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (07.12.1984), Article 32, available at <http://www.likumi.lv/doc.php?id=89648>.

transfer, transmitting, blocking or deleting, a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 200 [285 EUR] up to LVL 500 [711 EUR], on officials – from LVL 300 [427 EUR] up to LVL 500 [711 EUR], but for legal persons – from LVL 3000 [4,270 EUR] up to LVL 10 000 [14,230 EUR], with or without confiscation of the articles and tools used to commit the violation.

In the case of the blocking of a natural person's data, failure to follow an order regarding deletion or destruction of incorrectly or illegally obtained data, as well as of continuing to process a natural person's data after a permanent or temporary prohibition on processing has been specified, a fine shall be imposed on natural persons in an amount from LVL 50 [71 EUR] up to LVL 500 [711 EUR], on officials – from LVL 200 [285 EUR] up to LVL 500 [711 EUR], but for legal persons – from LVL 1000 [1,423 EUR] up to LVL 10 000 [14,230 EUR].'

- **Failure to Provide Information to a Data Subject.**

'In the case of failure to provide information specified by the law to a data subject a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 50 [71 EUR] up to LVL 500 [711 EUR], on officials – from LVL 200 [285 EUR] up to LVL 500 [711 EUR], but for legal persons – from LVL 1000 [1,423 EUR] up to LVL 5000 [7,110 EUR].'

- **Processing of a Natural Person's Data without Registration.**

'In the case of the processing of a natural person's data without registration specified by law or without the registration of the personal data protection specialist in the Data State Inspectorate, a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 100 [142 EUR] up to LVL 500 [711 EUR], on officials – from LVL 200 [285 EUR] up to LVL 500 [711 EUR], but for legal persons – from LVL 1000 [1,423 EUR] up to LVL 10 000 [14,230 EUR], with or without confiscation of the articles and tools used to commit the violation.

In the case of failure to submit persons to be registered data processing amendments that are specified by law to the Data State Inspectorate, a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 50 [71 EUR] up to LVL 400 [570 EUR], on officials – from LVL 100 [142 EUR] up to LVL 400 [570 EUR], but for legal persons – from LVL 800 [1,138 EUR] up to LVL 8000 [11,383 EUR].'

- **Failure to Provide Information to the Data State Inspectorate.**

'In the case of failure to provide the information provided for by the law or the provision of false information to the Data State Inspectorate, a

warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 50 [71 EUR] up to LVL 500 [711 EUR], on officials – from LVL 200 [285 EUR] up to LVL 500 [711 EUR], but for legal persons – from LVL 1000 [1,423 EUR] up to LVL 5000 [7,110 EUR].’

- **Failure to Accredit Persons at the Data State Inspectorate.**

‘In the case of failure to accredit the persons specified by the law at the Data State Inspectorate, a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 50 [71 EUR] up to LVL 500 [711 EUR], on officials – from LVL 200 [285 EUR] up to LVL 500 [711 EUR], but for legal persons – from LVL 1000 [1,423 EUR] up to LVL 5000 [7,110 EUR].’

- **Violation of the Prohibition on Sending Commercial Information.**

‘In the case of violation of the prohibition on sending commercial information as specified in the law, a warning shall be issued or a fine shall be imposed on natural persons in an amount from LVL 100 [142 EUR] up to LVL 350 [498 EUR], but for legal persons – from LVL 500 [711 EUR] up to LVL 5000 [7,110 EUR].’

- [84]. The institution responsible for examination of alleged violations of data protection foreseen by the Administrative Violations Code is the Data State Inspectorate; and its director, as well as employees authorised by him/her can take decision and impose an administrative sanction on behalf of the Data State Inspectorate.<sup>76</sup>
- [85]. There are no known cases where compensations have been paid to persons whose data protection was not observed, although there could in the future be cases where moral compensation would be requested.
- [86]. Other legal consequences are not foreseen by laws in data protection cases.
- [87]. If complaints are received or problems are identified in another manner by the data protection authority, the Data State Inspectorate carries out a control procedure which is set forth by the Administrative Procedure Law<sup>77</sup>, Law on Submissions,<sup>78</sup> and Latvian Administrative Violations Code.<sup>79</sup> If a violation of data processing has been detected the DSI adopts a decision with the purpose to ensure legality of data processing,

---

<sup>76</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (07.12.1984), Article 236<sup>10</sup>, available at <http://www.likumi.lv/doc.php?id=89648>

<sup>77</sup> Latvia/ Administratīvā procesa likums (25.10.2001), available at <http://www.likumi.lv/doc.php?id=55567>.

<sup>78</sup> Latvia/Iesniegumu likums (27.09.2007), available at <http://www.likumi.lv/doc.php?id=164501>.

<sup>79</sup> Latvia/Latvijas Administratīvo pārkāpumu kodekss (07.12.1984), Article 32, available at <http://www.likumi.lv/doc.php?id=89648>.



if necessary, by applying administrative sanctions. The laws related to data protection stipulate a wide range of powers of the DS in relation to prevention of violations (see in Chapter 2.1), for example, the DSI has a right to demand to block data, to destroy incorrect or illegally obtained data, to ban temporarily or permanently from processing data.

- [88]. In 2007, the Data state Inspectorate received and reviewed about 120 personal complaints on alleged violations of personal data processing. Approximately 30 of these were proven well-founded, and in 20 cases an administrative sanction was imposed: 16 administrative penalties for illegal data processing (two of them for illegal sensitive data processing) (from LVL 25/EUR 35 to LVL 750/EUR 1067); two warnings for a refusal to provide information to the data subject; a penalty of LVL 250 (EUR 355) for the operation of personal data processing system without registration, and a penalty for not providing information to the DSI.<sup>80</sup>
- [89]. As is evident from the numbers shown in annual reports of the Data State Inspectorate, enforcement of data protection legislation through sanctions payments in Latvia depends largely on the personal initiative of data subjects. Data subjects can get consultations by the DSI, as consulting is one of functions provided by the DSI on a regular basis. However, legal advice or legal representation is not provided by the DSI, and there are no effective NGOs in Latvia in the area of personal data protection.<sup>81</sup> Also there is no institutionalised system in Latvia for legal assistance and representation in data protection cases specifically. The financial risk of legal procedures in data protection cases is generally carried by individuals. Exceptions are set by the State Ensured Legal Aid Law which provides that '[t]he following persons have the right to legal aid: a citizen of Latvia; a non-citizen of Latvia; a stateless person; a European Union citizen who is not a citizen of the Republic of Latvia, but resides legally in the Republic of Latvia; a citizen of a state that is not a Member State of the European Union if he or she legally resides in the Republic of Latvia and has received a permanent residence permit; a person who has the right to legal aid ensured by the Republic of Latvia in accordance with the international agreement entered into by the Republic of Latvia; and an asylum seeker, a refugee and a person who has been granted the alternative status in the Republic of Latvia. [Those] persons have the right to legal aid if such persons, taking into account their special situation, state of property and income level, are unable to provide partly or fully for the protection of their rights. The Cabinet shall determine in which cases the special situation, state of property and income level of a person are being considered appropriate for the granting of legal aid. The State

---

<sup>80</sup> 2007. gada pārskats

<sup>81</sup> Interview with Ms Aiga Balode, official of the DSI, on 3 February, 2009.

shall ensure legal aid to any person who has obtained the status of a low-income or needy person. [Those] persons have the right to request legal aid and make amendments to the initial legal aid application’.

- [90]. Regarding the protection of personal data collected and processed in the context of employment the Personal Data Protection Law provides that ‘[t]he processing of sensitive personal data is prohibited, except in cases where [...] special processing of personal data, without requesting the consent of the data subject, is provided for by regulatory enactments, which regulate legal relations regarding employment, and such regulatory enactments guarantee the protection of personal data.’<sup>82</sup> The Labour Law provides that ‘[i]n order to select a prospective employee an employer has the right to transfer information obtained in accordance with [...] this Law, as well as the job application documents submitted by the applicant, only to the persons who, in the undertaking on behalf of the employer, prepare the decision regarding hiring of the employee. The information and documents referred to may be disclosed to third parties only with the consent of the applicant.’<sup>83</sup> ‘An employer may utilise the information regarding the state of health and occupational preparedness of an employee, obtained from an employee in accordance with [...] this Law, only if the taking of organisational, technological or social measures in the undertaking is required. An employer shall be responsible for ensuring the availability in the undertaking of the information referred to in Paragraph one of this Section only to persons who, as part of the tasks given to them by the employer, utilise such information for relevant organisational, technological or social measures.’<sup>84</sup> The Trade unions, however, have not been involved in activities regarding monitoring of compliance with the applicable legislation in that sector.

---

<sup>82</sup> Latvia/Fizisko personu datu aizsardzības likums (23.03.2000), Article 11, available at <http://www.likumi.lv/doc.php?id=4042> .

<sup>83</sup> Latvia/Darba likums (20.06.2001), Article available at <http://pro.nais.lv/naiser/textc.cfm?Key=0103012001062032772&Lang=03> .

<sup>84</sup> Latvia, Darba likums (20.06.2001), Article 93, available at <http://pro.nais.lv/naiser/textc.cfm?Key=0103012001062032772&Lang=03> .

## 5. Rights Awareness

- [91]. In addition to the Eurobarometer surveys on data protection, two more surveys have been conducted in 2005 and 2003.
- [92]. In 2005 a public opinion poll on personal data protection was conducted. 1007 permanent residents of Latvia (age 18-74) were polled, based on random stratification (1014 respondents in 2003). More than a half (52.9 per cent) of the respondents considered that their personal data which are held by institutions are only partly protected against the possibility to be obtained by unauthorised persons or institutions (41.9 per cent in 2003). Only 7.2 per cent of respondents were sure that their data are secure (10.9 per cent in 2003).
- [93]. 10-20 per cent of respondents had encountered various problems with regard to personal data processing or security. 19.5 per cent of respondents report having been in situation where their data have been processed incorrectly, thus allegedly creating financial or moral damages. In comparison to the survey of 2003, that number has slightly increased (14.5 per cent in 2003).
- [94]. 13.5 per cent of respondents report having faced a situation where they have been requested to provide more data about themselves than necessary in a particular situation. In comparison to the survey of 2003 that number has doubled (6.4 per cent in 2003).
- [95]. 13.4 per cent of respondents report suffering damages as their personal data have been obtained by a third party who has used them in order to gain material benefit. In comparison to the survey of 2003, that number is lower (20.7 per cent in 2003).
- [96]. Almost a third of respondents (29.5 per cent) were aware about the existence of the data state Inspectorate. In 2003 that number was 23.3 per cent.
- [97]. 22.9 per cent of respondents have tried to obtain information about themselves from institutions or companies. Most of them (66.2 per cent) did it successfully, although 32.5 per cent of respondents were refused the information.
- [98]. The results of the survey were interpreted as showing that awareness about the data protection should be raised for state administration institutions, as well as for the public in general.

## 6. Analysis of deficiencies

- [99]. As the report shows, an important deficiency regarding effective data protection and effective relevant institution is the lack of institutional independence of the Data State Inspectorate. Although this concern has been discussed already for some years and a draft law has been prepared by the Data State Inspectorate, there is no information on when the status of the DSI could be changed.
- [100]. As the Data State Inspectorate is responsible for the implementation and observance of all Latvian legislation concerning data protection, as well as freedom of information, both of which are complicated topics and need much awareness raising, the DSI cannot provide enough of proactive work with its existent capacity. However, as a result of the period of economic problems in the state, staff has been reduced by five employees and the budget for 2009 is set at the same level as in 2003.
- [101]. The legislative framework is worked out in order to implement the EU legislation and international standards regarding the data protection, but, as the DSI has limited resources, controlling of implementation of legislation cannot be considered as sufficient.
- [102]. In the implementation of the control function it would be important to take into account that some of laws affecting personal data protection contain rather vague provisions, which can be interpreted differently from case to case. For example, the Population Register Law states that a third party can obtain information about the person from Population Register on basis of a 'reasoned submission',<sup>85</sup> but no explanation is provided on what reasons are to be considered valid. The Regulation of the Cabinet of Ministers on General Security Requirements of State Information Systems<sup>86</sup> states that 'The system manager shall implement system security measures according to State budget resources granted for this purpose', and a similar statement is included in Regulation of Cabinet of Ministers General Technical Requirements of State Information Systems: 'The system manager shall ensure the implementation of the requirements specified in these Regulations according to the State budget resources granted for this'.<sup>87</sup> It is thus not

---

<sup>85</sup> Latvia/Iedzīvotāju reģistra likums (27.08.1998), Article 19, available at <http://www.likumi.lv/doc.php?id=49641>.

<sup>86</sup> Latvia/Ministru kabineta noteikumi Nr. 765 'Valsts informācijas sistēmu vispārējās drošības prasības' (11.10.2005), Point 22, available at <http://www.likumi.lv/doc.php?id=118990>.

<sup>87</sup> Latvia, Ministru kabineta noteikumi Nr. 764 'Valsts informācijas sistēmu vispārējās tehniskās prasības' (11.10.2005), Point 10, available at [http://www.eps.gov.lv/files/juridiskabaze/likumi/MKnot\\_764\\_vistehnpras.doc](http://www.eps.gov.lv/files/juridiskabaze/likumi/MKnot_764_vistehnpras.doc).

clear from those texts how the lack of sufficient resources affects the observance of the necessary requirements of data protection.

- [103]. Although the Data State Inspectorate imposes administrative penalties and engages in court cases if those decisions are appealed in administrative court, there is quite low awareness of those cases and the consequences of violations of data protection legislation.

## 7. Good practices

NTR.

## 8. Miscellaneous

NTR

.

# Annexes

## Annex 1 – Tables and Statistics

	2000 <sup>88</sup>	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	-	LVL 100,182 [EUR 142,546]	LVL 100,182 [EUR 142,546]]	LVL 370,000 [EUR 526,463]]	LVL 602,712 [EUR 857,582]  (LVL 282,748 from the State budget; LVL 218,314 Phare	LVL 587,274 [EUR 835,616]  (LVL 266,704 from the State budget; LVL 293,070 Phare	LVL 373,908 [EUR 532,023]  (LVL 305,349 from the State budget; LVL 66,759 Phare financing)	LVL 500,049 [EUR 7011,506]]

<sup>88</sup> The Data State Inspectorate was established in 2001.



					financing)	financing)		
--	--	--	--	--	------------	------------	--	--

Staff of data protection authority	-	10 (+5 employees on temporary contract basis for performance of particular tasks)	13	17	20	18	23	24
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	-	0	2	12	0	3	0	7
Number of data protection registrations	-	2767	6785	1646	705	625	731	769 + 182 personal data

								processing registrations <sup>89</sup>
--	--	--	--	--	--	--	--	---

---

<sup>89</sup> According to amendments of 1.03.2007 to the Personal Data Protection Law, since 1.09.2007. the data processing shall be notified to to the Data State Inspectorate instead of notification of system.

Number of complaints received by data protection authority	-	38	86	83	136	168	133	120
Number of complaints upheld by data protection authority	-	11	56	33	42	37	21	30
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)	-	Warnings and opinions; no sanctions imposed	Warnings and opinions; no sanctions imposed	8 administrative penalties (7 fines, 1 warning); 1 legal duty to block the data processing	2 administrative penalties (fines)	11 administrative penalties (10 fines, 1 warning)	20 administrative penalties (16 fines, 4 warnings)	

				system				
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)	-	No information	No information	No information	No information	No information	No information	No information
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation )	-	No information	No information	No information	No information	No information	No information	No information

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

## Annex 2 – Case Law<sup>90</sup>

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

<b>Case title</b>	
<b>Decision date</b>	2008-07-01
<b>Reference details</b> (reference number; type and title of court/body; in original language and English [official translation, if available])	Case No.A42342405, Administratīvā apgabaltiesa [Administrative Regional Court]
<b>Key facts of the case</b> (max. 500 chars)	In October 2004 the National Mental Health Agency included personal data on O.B. in the National Register (Register) of Psychiatric Disorders and Psychiatric Illnesses based on diagnostic information supplied by the doctor in charge of O.B.'s health care. In addition to the inclusion of sensitive health data in the form of a diagnosis, the doctor had supplied the incorrect diagnose code, which corresponded to a more serious illness than that O.B. had been diagnosed with on 2004-12-04. O.B. requested the Ministry of Health to erase his sensitive data from the Register and to compensate him for the harm done. The Health Ministry informed O.B. that his application would be reviewed within 4 months. O.B. data processing was terminated through a decision by the Ministry of Health on 2005-06-02.

<sup>90</sup> After repeated requests to provide decisions or court decisions for needs of the report, the Data State Inspectorate has answered that it will not provide full texts of the decisions, as they contain personal data of persons involved, and erasing of personal data will take a lot of time. Suggestion was to use information provided on cases in the annual reports of the Data State Inspectorate, however, that information is far too short to fulfill requirements for this Annex.

<p><b>Main reasoning/argumentation</b> (max. 500 chars)</p>	<p>The Administrative Regional Court reaffirms that the illegal storing of information on O.B.'s diagnosis constitutes illegal processing of O.B.'s sensitive personal data, and illegal processing of sensitive data, especially data concerning health status, in itself is a serious violation of a person's right to private life. The illegality of the data processing is not contested in this case and was recognized by the Ministry of Health decision to terminate the said processing. However, the Court established that the moral harm to O.B., which entailed suffering and anxiety, cannot adequately be compensated by the termination of the illegal activity, especially since this was not timely, nor by the written apology by the responsible institution and the Court awarded 3000 LVL to the claimant as compensation for moral damage, 1500 LVL for the Agency's illegal processing of data, for which O.B. suffered moral harm, and 1500 LVL for the Ministry of Health's unreasonably slow review of the case which prolonged the harm by six months.</p>
<p><b>Key issues (concepts, interpretations) clarified by the case</b> (max. 500 chars)</p>	<p>The Court argued that although the illegal processing of the claimant's personal data, which violated the claimant's right to private life, was uncontested by all parties and recognized through the Ministry of Health decision that terminated the illegal data processing, the fact that the claimant's case was not reviewed in a timely manner, which resulted in the continuation of the illegal data processing for six months after the claimant's request to remove it, allowed the violation to continue for this period of time. The Ministry of Health unfounded slowness in reviewing the case is an infraction in itself. Contrary to previous review by a court of this case, where termination of the illegal data processing was ruled adequate response by the authorities, this ruling establishes the right to damages for moral harm for anxiety caused by illegal processing of sensitive personal data.</p>