

TABLE OF CONTENTS

| | |
|--------------------------------------------------------------------------------------------------------|----|
| Report of Signe Plūmiņa, Director of the Data State Board..... | 2 |
| 1. Basic Functions and Obligations of the Data State Inspection..... | 5 |
| 2. Activities of the Data State Agency in the Development of Regulatory Acts and Policy Documents..... | 7 |
| 3. Registration of Personal Data Processing Systems | 19 |
| 4. Complaints on Violations in Personal Data Processing | 20 |
| 5. Conclusions and Explanations..... | 22 |
| 6. Participation of the Data State Inspection in Proceedings..... | 50 |
| 7. Audit and Auditors of Personal Data Processing | 51 |
| 8. Public Information and Social Activities | 53 |
| 9. International Activities of the Data State Inspectorate..... | 56 |
| 10. Phare 2002 Twinning Project Data State Inspection..... | 74 |
| 11. Information on the Use of Budget Funds | 80 |
| 12. Education and Training of Employees of the Data State Inspection..... | 83 |
| 13. Main Tasks and Planned Activities in 2006 | 89 |

Report of Signe Plūmiņa, Director of the Data State Board

The 20th century is being referred to as a century of democracy; at the same time, new threats to democracy due to which the privacy of an individual is restricted appear. Privacy, or the right of an individual to be left alone and undisturbed, is threatened and restricted in many ways in our days. Privacy has been restricted by the so-called war against terrorism, which restricts the freedom of an individual, including privacy, even in countries that were regarded as the strongest supporters of human rights.

Many countries have showed increased interest and collected additional information on their residents. Often it is done without their consent. An example of such collection of information was seen in the telecommunications sector, when law enforcement authorities requested information on the calls made by and the location of an individual. It was the issue of traffic data that was one of the most disputed within the European Union in 2005; for the opinions of law enforcement institutions and human right institutions and the interests of telecommunication service providers clashed in this context. Therefore, in the EU, it is being discussed about data protection issues under the third pillar, which are related to law enforcement institutions.

The year 2005 has been a special year as regards data protection. Ten years have passed since Directive 95/46 EC entered into force. During the ten years a lot has changed, and EU member states more and more often express the opinion that it is necessary to amend the Directive in order to make it compliant with the present conditions brought about by the development of modern technologies and in relation to the changes brought about in our everyday life by globalisation processes.

Data protection issues have become topical in many spheres, also in the tourism industry – increased attention is paid to the identity control of travellers, especially in the countries that have faced the damaging consequences of terrorism. In some cases it is an obligatory requirement to take fingerprints of

travellers, which normally was applied only to suspected persons (especially when travelling to the USA). There are discussions on the implementation of passports with biometrical data in the European Union. All these trends influence the personal data protection also in Latvia. Therefore, this issue becomes more and more current in Latvia and the European Union. In 2005, the Data State Inspection continued to implement the functions specified in the legal acts and took part actively in the working groups connected with the protection of personal data both on the national and on the European Union level. The implementation of European Union Phare Twinning Project No.LV/2002/IB/OT- 01 'The Data State Inspection', which was commenced in 2004, has been brought to an end. The main objective of the project was to strengthen the administrative capacity of the Data State Inspection and to prepare a future development model of the DSI as an independent institution. In the European Union there is not a single model of data protection institutions; therefore the practice is different in European Union countries. There are only a few data protection authorities (e.g. in the UK, Hungary) that are also responsible for the supervision of the implementation of the legislation on freedom of information. In this context, also in Latvia the main issue is the balance between freedom of information and data protection.

I would like to point out that the main task of the Data State Inspection is to achieve that the Personal Data Protection Law is compliant, easy-to-understand and pragmatic. The Data State Inspection has not been established to hinder the development of businesses or the work of public administration authorities in Latvia but to provide support in order to develop good practices of data protection. Therefore, it will be an important task in the next year to educate people on issues related to personal data protection and freedom of information, and it has been also included in the Strategic Development Plan 2004-2007 of the Data State Inspection. I am convinced that, if people are better informed on their rights, they will be able to protect their privacy much better and will know in what situations they have the right to receive information from

public administration authorities. Therefore, it is important to provide relevant information to people on their rights and obligations.

The compliance with the principles of personal data protection is important already from the initial development stage of the legislation; therefore, in 2005 the Data State Inspection prepared opinions on drafts of a number of regulatory acts, including the Regulations on the Agreement on cooperation in combating terrorism, organized crime and illicit trafficking in narcotic and psychotropic substances and precursors, and other crimes between the Republic of Latvia and the Republic of Slovenia, the Amendments to the Human Genome Research Law, Patient Rights Law, the Amendments to the Judiciary Law etc.

In conclusion, I would like to thank those people who contacted the Data State Inspection and notified us on possible violations or to receive consultations about issues that are within the scope of competence of the DSI. Also, I would like to thank all employees of the DSI, especially those who have been working with it since its establishment.

Signe Plūmiņa

1. Basic Functions and Obligations of the Data State Inspection

The Data State Inspection (hereinafter – the DSI) is a state administration authority, which is subordinate to the Ministry of Justice; the work of the DSI is regulated by Cabinet Regulations No. 408 of 28 November 2000 Regulation of the Data State Inspection. In 2005, the Regulations of the DVI were developed and approved; the Regulations set out the structure and work organisation of the DSI (the Regulations can be found on the website of the DSI – <http://www.dvi.gov.lv>).

The DSI commenced its work in 2001, and its functions are specified under the Personal Data Protection Law, the Electronic Documents Law, and the Freedom of Information Law.

In supervising the compliance with the Personal Data Protection Law, the DSI acts independently. Decisions taken by it may be appealed only to court.

Obligations of the DSI in relation to personal data protection:

1) to ensure that the processing of personal data is performed in compliance with the Personal Data Protection Law;

2) to take decisions and deal with complaints related to personal data protection;

3) to register personal data processing systems;

4) to propose and carry out actions that are aimed at more efficient personal data protection and provide opinions on the compliance of personal data processing systems developed by government and local government institutions with the requirements of regulatory acts.

5) together with the Directorate General of Latvia State Archives, to take decisions on the transfer of personal data processing systems to state archives for keeping;

6) to accredit persons who want to carry out system audits of personal data processing systems of government and local government organisations in accordance with the procedure approved by the Cabinet of Ministers.

Obligations of the DSI in relation to electronic documents are:

- 1) to accredit certification service providers in accordance with the principle of voluntary accreditation;
- 2) to control that reliable certification service providers comply with the regulations on the provision of certification services;
- 3) to compile a list of experts who have the right to carry out security tests of information systems, equipment and procedures used to provide certification services;
- 4) to monitor that the e- signature control data and time stamp registers of qualified certificates issued, cancelled, suspended and renewed by reliable certification service providers are continuously available on-line.

As to freedom of information, the obligation of the DSI is to monitor the compliance with the Freedom of Information Law in accordance with the procedure set out in the regulatory acts.

2. Activities of the Data State Agency in the Development of Regulatory Acts and Policy Documents

To ensure the compliance of the regulatory acts of the Republic of Latvia to the requirements of the European Union in relation to personal data protection principles, the DSI in 2005 prepared a number of draft regulatory acts and took part in working groups that prepared draft regulatory acts and policy documents.

Amendments to the Constitution of the Republic of Latvia

In 2005, pursuant to the task specified in Prime Minister's Order No. 484 of 24 October 2003 On the working group for the preparation of draft regulatory acts that are required for the determination of the status of independent institutions – to prepare draft legal acts that are required to regulate the status of independent institutions and that were to be submitted to the Cabinet by the Minister of Justice – the Concept was developed.

The Concept says that the possible place of the so called independent institutions in the constitutional and administrative state system of Latvia has to be assessed in the context of the competence of the institutions. The working group carried out a comprehensive analysis of the powers of the de facto independent institutions of Latvia, analysing in every individual case the need for independence of the particular institution to carry out its functions.

The working group studied the regulations on the independent state administration institutions of Latvia in laws, their functions, institutional structure, funding mechanism and independence justification (i.e. the necessity to be outside the subordination system to the Cabinet) required for them to carry out their functions efficiently.

The working group identified the existing independent institutions of Latvia that are not subordinate to the Cabinet and that could not realise their functions or it would be too inefficient if they were subordinate to the Cabinet in accordance with Section 58 of the Constitution.

The working group's opinion is that the exemption of the institutions specified in the Concept from the general subordination system to the Cabinet to ensure that the said institutions could fulfil their functions efficiently is justified.

Considering the task to develop a precise regulation of independent institutions as a special type of direct state administration institution in the legislation and to provide a justification therefor in the Constitution, the following amendments to the legislation are required:

1. amendments to the Constitution of the Republic of Latvia
 1. a draft law on amendments to the State Administration Structure Law;
 2. a draft law on the right of independent institutions to issue external regulatory acts;
 3. a draft law on amendments to the Law on the Proclamation, Coming into Force and Validity of Laws and other Acts Adopted by the Saeima (Parliament), the President and the Cabinet of Ministers;
 4. a draft law on amendments to the Administrative Procedure Law;
 5. amendments to the laws that regulate independent institutions (including laws that regulate the status, functions, rights and obligations of the DSI).

Furthermore, the European Commission, having assessed the legislation of Latvia in force, concluded that Latvia has not implemented the requirement under Article 28 of Directive 95/46/EC in relation to the functional independence of the supervising authority of personal data. Upon Prime Minister's order, a working group was created on January 10, 2005; its task was to prepare and submit to the Cabinet the required draft legal acts in order to ensure the compliance of legal acts of Latvia to the requirements laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of

personal data and on the free movement of such data, as well as to establish the basic principles of the work of personal data supervision institutions.

The working group, pursuant to Cabinet Order No. 322 of 18 May 2005 On the Concept for the Regulation of the Status of Independent Institutions prepared the draft law Amendments to the Personal Data Protection Law. Furthermore, the working group reached an agreement on the necessity to prepare the Data State Inspection Law, which, like all the other regulatory acts on the work of the institutions specified in the Concept, will be passed to the Parliament after the adoption of the amendments to the Constitution of the Republic of Latvia.

Amendments to the Criminal Law

Violations in processing of personal data are subject to administrative liability, and the penalty imposed can be a warning, a fine, suspension of the operation of the personal data processing system, forfeit of the used technical equipment.

In 2005, with the purpose to facilitate the protection of personal data and to prevent illegal processing of personal data, the work was commenced to stipulate criminal liability for violations of personal data processing. The application of criminal liability for illegal data processing is justified if:

1. personal data are processed illegally and if appropriate technical and organisational means are not used in personal data processing to protect personal data and prevent illegal processing thereof and if human rights are infringed due to the said (Section 96 of the Constitution);
2. the existing criminal liability as stipulated by the Criminal Law for intended disclosure of personal secrets of other persons not always is proportional to the seriousness of the violation and the damage incurred and not always it is a sufficiently efficient penalty (the

penalty that can be applied to violations related to personal data processing is custody or forced labour, or a penalty of up to 20 minimum monthly wages). This penalty is not adequate in cases when information is disclosed from, for example, bank information systems, government information systems, including patient registers (HIV/AIDS State register, Psychological Disorder and Psychological Illnesses State Register, Sexually Transmitted and Contagious Dermatologic Diseases State Register, Drug Addict Patients State Register and other registers).

Amendments to the Personal Data Protection Law

In 2005, the DSI drew up the draft law Amendments to the Personal Data Protection Law. The purpose of the said draft law was to specify the personal data processing systems to be registered and the registration procedure thereof, to specify individual legal norms that previously had proved to be problematic in the application of the Law, and to specify the requirements of Directive No. included in the Personal Data Protection Law, inter alia those related to the status of the DSI. The draft law conforms to the requirements of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The draft law stipulates that:

1. a draft law on the functions, tasks and competences of the DSI shall be prepared. The adoption of the Law on the DSI depends also on the amendments to the Constitution of the Republic of Latvia in relation to the subordination of government institutions to the Cabinet of Ministers, which need to be made. The necessity of an individual law on the DSI is connected also with other its functions – in relation to the supervision pursuant to the Freedom of Information Law and the

Electronic Communications Law. Since the DSI has a number of functions the fulfilment of which is to a great extent connected also with the supervision of the activity of public legal subjects in certain spheres, the regulation of its status in one law will not provide the legal regulation required for the scope of its competences.

2. The draft law stipulates that the Cabinet Regulations by which the following forms will be approved shall be issued: personal data processing system registration application; application on changes in personal data processing system; application of the responsible person of the system controller; and application on the exclusion of the personal data processing system from the register of personal data processing systems. The said Cabinet Regulations are required because at the present the information to be submitted pursuant to Section 22 of the Personal Data Protection Law may be submitted in a free form, which makes the registration process difficult, and because in accordance with Section 72 of the State Administration Structure Law an internal regulatory act issued by a state institution is binding only to the institution (its structural unit, employees or officials) to which the regulation applies.
3. It is planned to charge a fee for the registration of responsible persons with the DSI.
4. It is planned to prepare Cabinet regulations that would specify the procedure of training of personal data protection specialists.
5. It is planned to prepare Cabinet Regulations by which the standard form of the agreement on the transfer of personal data will be approved.

Amendments to the Freedom of Information Law

Since a number of current amendments are required to the Freedom of Information Law in order to ensure the efficiency of Cabinet Regulations No. 280 of 26 April 2005 on the procedure whereby internal information is protected, which was prepared by the working group headed by the Constitution Protection Bureau, in order to implement Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, the Secretariat of the Minister of Special Assignments for Electronic Administration has prepared a draft law on the amendments to the Freedom of Information Law. The amendments are required also to update a number of provisions of the Law in accordance with the Committee of Ministers of the European Council Recommendation No. R (2002) 2 of 21 February 2002 on the access to official documents; therefore, the DSI proposed to assess the possibility to establish an inter-institutional working group whose task would be to align the provisions on freedom of information and accessibility to information in accordance with Sections 100 and 104 of the Constitution of the Republic of Latvia and other regulatory acts.

Patient Rights Law

Pursuant to the decision of the Social and Labour Affairs Committee, the DSI in June 2005 was asked to delegate a representative to the working group whose task was to prepare the draft Patient Rights Law. The objective of the Patient Rights Law is to protect the less powerful party in the doctor-patient relationship, i.e. the patient. Therefore, a clear, easy-to-use and understand law that would cover the spheres in which protection by law is necessary was required. At the moment, the preparation of the draft law has been suspended because the scope of its implementation and application is not fully clear. However, the DSI also in future will be invited to and will take part willingly at the working group in order to ensure that the draft law is passed to the Parliament of the Republic of Latvia.

Amendments to the Administrative Code of the Republic of Latvia

In June 2005, the DSI, within the scope of its competence, assessed the draft law Amendments to the Administrative Code, which had been prepared by the Ministry of Economy; it expressed a number of objections on the draft law in connection with a number of issues that are within the competence of the DSI.

The DSI did not approve the draft law Amendments to the Administrative Code because the DSI had been specified therein as the responsible institution which handles administrative cases connected with unrequested commercial messages because it does not conform to the competence assigned to the DSI under the Personal Data Protection Law. The DSI pointed out that cases when unrequested commercial messages violate personal data protection are very rare, i.e. if the e-mail address contains personal data (any information on an identified or identifiable physical person). In accordance with Article 8.2 of the Personal Data Protection Law, e-mail addresses are not sensitive personal data (personal data which indicate the race, ethnic origin, religious, philosophical or political convictions, or trade union membership of a person, or provide information as to the health or sexual life of a person).

Since unrequested commercial messages are connected with commercial activities (including compliance with consumer rights), in its opinion the DSI pointed out that the issue included in the draft law is not within its competence and that it is impossible to fulfil this function within the existing capacity of the DSI.

Regulations on the procedures for the preparation, drawing up, storage and circulation of electronic documents in State and local government institutions, and the circulation procedures between State and local government institutions, or between these institutions and natural persons and legal persons

On June 27, 2005, the Cabinet approved the Cabinet Regulations on the procedures for the preparation, drawing up, storage and circulation of electronic documents in State and local government institutions, and the circulation procedures between State and local government institutions, or between these institutions and natural persons and legal persons.

The Regulations set out:

1. The procedure for the preparation and drawing up of electronic documents, except electronic documents drawn up by natural and legal persons if the documents are not intended for submission to state or local government institutions;
2. File formats to be used for electronic documents;
3. The procedure of circulation of electronic documents between state and local government institutions and between the said institutions and natural or legal persons;
4. A possibility to make a written agreement on the use of electronic signature in electronic documents;
5. That the circulation of electronic documents is ensured through electronic mail and by using specially designed on-line forms of state and local government institutions or other electronic data carriers;
6. The procedure of storage of documents by state and local government institutions until their transfer to the state archive for storage.

In accordance with the said regulations and pursuant to Article 6.4 of the Electronic Documents Law, state and local government institutions have to develop instructions on the internal circulation of electronic documents. The Development and Analysis Department of the DSI has commenced the preparation of the said instruction.

The most essential new provision is the possibility to agree on the use of electronic signature in electronic documents. The said agreement will allow avoiding the requirement for a secure electronic signature. If the agreement

exists, electronic documents do not need to contain all the details required under the law and also the provisions of the law referred to in Paragraph 3 of the Regulations may not be applied.

Regulations on technical and organisational requirements for qualified certificates, reliable certification service providers, secure means of generation of electronic signatures and the procedure of secure verification of electronic signatures

On July 12, 2005, the Cabinet approved the Regulations on technical and organisational requirements for qualified certificates, reliable certification service providers, secure means of generation of electronic signatures and the procedure of secure verification of electronic signatures.

The basis of the requirements of the Regulations are: National Standards of the Republic of Latvia LVS ETSI TS 101 456 V 1.2.1:2004 and LVS ETSI TS 102 023 V 1.2.1:2004, which are binding to reliable certification services providers and which will be used by special experts to assess potential reliable certification services providers in accordance with Cabinet Regulations No. 357 and No. 358 of July 1, 2003; National Standards of the Republic of Latvia LVS CWA 14167-1:2004, LVS CWA 14167-2:2004 and LVS CWA 14169:2004, which implement the requirements of Directive 1999/93/EC, Annexes 2 and 3, in accordance with European Commission Decision No. 2003/511/EC of July 14, 2003; National Standard of the Republic of Latvia LVS CWA 14171:2004, which is related to secure verification of electronic signatures; National Standard of the Republic of Latvia LVS ISO/IEC 17799, National Standard of the Republic of Latvia LVS ISO/IEC TR 13335-1, 2, 3, National Standard of the Republic of Latvia LVS ISO/IEC 12207, which will be used by special experts to assess the conformity of potential reliable certification services providers in accordance with Cabinet Regulations No. 357 of July 1, 2003 on the information to be provided in

security descriptions of information systems, equipment and procedures used for certification services and Cabinet Regulations No. 358 of July 1, 2003 Procedure and time limits for the testing of information systems, equipment and procedures used in certification services .The draft regulations were prepared by a working group composed of representatives of the DSI, the Latvian Association of Information Technologies and Telecommunications, the Information Society Bureau, the Post of Latvia, the State Information Network Agency, the State Revenue Service, the Association of Local Governments of Latvia, the Department of Citizenship and Migration Affairs, the Financial and Capital Market Commission.

Amendments to Cabinet Regulations No. 25 of 13 January 2004 Procedure for the accreditation of persons who wish to perform system auditing of data processing systems of government and local government institutions.

On October 11, 2005. pursuant to Paragraph 3.6 , Section 29 of the Personal Data Protection Law, amendments were made to Cabinet Regulations No. 25 of 13 January 2004 Procedure for the accreditation of persons who wish to perform system auditing of data processing systems of government and local government institutions.

The amendments provide for an additional provision to be included in the Regulations – persons may apply for the accreditation by the DSI if they have not sentenced for intended offences, have been rehabilitated, or the conviction has been extinguished or set aside. If the system auditor has provided untruthful information in order to get the accreditation certificate, the person will be punished pursuant to the Administrative Code or the Criminal Code. Furthermore, the amendments stipulate that Chapter VIII of the Regulations will be deleted.

Cabinet Regulations on the Transfer and Storage of Traffic Data of Certain Amount

In 2005, the DSI provided a number of opinions on the draft Cabinet regulations regarding the transfer and storage of traffic data.

The European Council adopted the declaration on combat against terrorism on March 25, 2004, pursuant to which the legal instrument on the keeping of data had to be implemented until June 2005. France, Ireland, Sweden and the United Kingdom developed the Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism (hereinafter – the Framework Decision).

The purpose of the draft Framework Decision was to facilitate the legal cooperation under criminal cases by similar legal acts that contain similar legal norms in all Member States, including information on the storage of data that has been processed and stored by public providers of electronic services or which have been transmitted in the electronic communications network in order to investigate, disclose and punish criminal offences, inter alia terrorism.

Latvia supports the development of an instrument that would regulate data retention and storage issues on the level of the European Union; for at the present there are not any common principles of data retention and storage within the EU that would facilitate the cooperation among law enforcement institutions in combating crime (Latvian position) and, as a member state of the EU, it also is taking part in the development of the said document. It is planned to adopt the Framework Decision until the end of 2005.

General Technical Requirements for Government Information Systems

In accordance with Section 4 of the State Information Systems Law, which stipulates that a user, natural or legal entity, of a state information system who has concluded an agreement with the system controller on the use of data or who receives data from the controller of the state information system on the basis of application or pursuant to the procedure set out in regulatory acts, Cabinet Regulations No. 764 and 765 General Security Requirements for State Information Systems were adopted on October 11, 2005.

The Regulations specify the general technical requirements for state information systems. The general requirements for state information systems are complied with in the management of system information and technical resources. The Security Department of the DSI has commenced implementing the said regulations.

Schengen Information System

To establish and assess the tasks to be fulfilled in order to align the national legislation with the acquis provisions of Schengen, S. Plūmiņa, Director of the DSI, took part in the working group of the Ministry of the Interior in relation to the implementation of the said regulations, i.e. in the preparation of the draft Schengen Information System Law.

It is planned that the working group will prepare a draft regulatory act, which stipulates that the DSI is the institution responsible for personal data protection within the Schengen Information System. Also, the DSI has submitted to the Ministry of Justice the Twinning Light project application 'Support to the DSI in the Supervision of Personal Data Protection in Relation to the Schengen Information System and the Europol Information System' with the purpose to ensure the implementation of the requirements of the Schengen Convention and the Europol Information System in the Republic of Latvia in compliance with the requirements of the EU.

3. Registration of Personal Data Processing Systems

The DSI performs the registration of personal data processing systems. Section 21 of the Personal Data Protection Law stipulates that 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, and establish systems for personal data processing, shall register such in accordance with the procedures prescribed in this Law unless otherwise prescribed by law.

Prior to registration, the systems to be registered shall be subject to control, during which the conformity of the system to the Personal Data Protection Law is assessed on the basis of the information provided; in addition, the internal regulations on information system security, system audit conclusions and other documents that describe data processing and protection processes in the system may be demanded.

Until the end of 2005, in compliance with the requirements under Chapter IV of Personal Data Protection Law, more than 12,000 personal data processing systems had been registered with the DSI.

The fact that the number of the changes to be registered in accordance with Personal Data Protection Law grew substantially in 2005 characterises well the topicality of the understanding on personal data protection. Compared to 2004, the number of changes registered grew by 50%. This shows that controllers of personal data processing systems do not grow inactive after the first registration; instead, they follow actively the changes in data processing and system operation.

In the reporting period, 625 systems had been registered with the DSI. The amount of state duty collected was 12,977 lats. In 2005, the Control and Registration Department provided more than 1,500 consultations on the registration of systems and the legal aspects of development and operation of processing systems.

4. Complaints on Violations in Personal Data Processing

The DSI supervises over personal data protection by fulfilling the functions specified in regulatory acts, adopting decisions and issuing regulatory acts in compliance with the legislation. One of the obligations of the DSI is to examine complaints and adopt decisions in relation to personal data protection. Like in previous years, personal data protection has been the most significant function of the DSI, which in most cases has been based on complaints from individuals on possible infringement of privacy.

To examine submissions or complaints, the DSI carries out controls and, if violations in personal data processing are detected, it adopts decisions with the purpose to ensure the legality of personal data processing, applying, if necessary, administrative sanctions under individual cases. The controls carried out by the DSI prevents illegal processing of personal data by ensuring that the regulatory norms in relation to personal data protection are complied with and by facilitating the knowledge of the public on personal data protection in Latvia.

In 2005, the Control Department of the DSI carried out 168 controls on possible violations of Personal Data Protection Law. Judging by the complaints received and the controls carried out by the DSI in the past year, in 2005 the most frequent violation of the law was personal data processing without legal justification, i.e. data processing without data subject's consent therefor, data processing not specified under contractual relationships with the data subject etc.

To establish whether a violation has been committed, the DSI carries out controls and, if violations in data processing are detected, adopts decisions with the purpose to ensure the legality of personal data processing, applying, if necessary, administrative sanctions. The Personal Data Protection Law stipulates a wide range of powers of the DSI in relation to the prevention of violations. The DSI has the right to demand that data be blocked, that incorrect or illegally obtained data be deleted or destroyed, or set a temporary or permanent ban on

data processing. Furthermore, upon relevant submission from the data subject, the DSI has the right to carry out a control in order to check the conformity of personal data processing to the requirements of regulatory acts in cases when the system controller has provided data if it is prohibited pursuant to the law.

The procedure whereby submissions and complaints of persons are handled is set forth in the Administrative Procedure Law (in force as of 1 February 2004), unless a different procedure is stipulated by special legal norms under other laws (e.g. Code of Administrative Violations of Latvia, Law on the Procedure whereby Submissions, Complaints and Proposals are Examined by State and Local government Institutions).

Judging by the complaints received and the controls carried out by the DSI, the most frequent violation of the law has been the processing of personal data without legal justification.

5. Conclusions and Explanations

On personal data processing in notices of violation and decisions of officials of the State Police on administrative traffic violations committed by physical persons

In 2004, pursuant to a submission from a physical person, the DSI commenced the control, which was brought to an end in 2005; in the control the proportionality of the processed personal data to the purpose of personal data processing in relation to notices of violation and decisions of officials of the State Police on administrative traffic violations committed by physical persons was assessed.

In accordance with Article 248.1 of the Administrative Violations Code of Latvia (hereinafter -AVCL), notices of administrative violations should specify: time and place of issue; position, name and surname of the officer; place, time, and substance of the administrative violation; the regulatory act which stipulates liability for the violation; names and addresses of witnesses or victims, if any; explanation of the violator; other information required to make a decision; whereas in accordance with Article 248.2 of the AVCL the following data on the violator are to be included in notices of violation: name and surname, year and place of birth, place of employment, job or position, place of residence, and other data relevant for the examination of the administrative violation. The notion 'other data' used in the Section should be interpreted in accordance with the purpose of processing of personal data. For example, in respect to administrative detention it is stipulated in Section 31 of the AVCL that administrative detention may not be applied to pregnant women, women with children up to twelve years of age, persons under eighteen years of age, and first and second category disabled persons. In accordance with the restrictions on the application of administrative detention to certain groups of persons as stipulated in Section 31 of the AVCL, in cases when the administrative penalty applied

under the administrative violation pursuant to the respective Section of the AVCL (e.g. 46, 155³, 155⁴) can be administrative detention, the State Police has the right to demand from the person information in order to establish whether the application of the said administrative penalty is not subject to any restrictions (that is, the information requested is of significance in connection with the examination of the administrative case and the said conforms to the purpose of personal data processing).

Furthermore, Article 32.2 of the AVCL stipulates that the character of the violation committed, violator's personality, degree of guilt, property status, and aggravating or mitigating circumstances should be considered in the determination of penalty.

Therefore, the provision of such personal data which are not to be provided in accordance with the purpose of personal data processing and in accordance with the norms of the AVCL but which however might influence the type and amount of the administrative penalty to be applied is a right, not an obligation, of the person, i.e. in order for the person to realise his/her rights provided for in the AVCL.

On the basis of the said, the amount of information requested (on the number of dependants) is proportional to the purpose of personal data processing upon condition that it is of significance in examining the administrative violation case (e.g. to find out whether the application of the administrative penalty is not subject to any restrictions) or if the violator provides the information in order to realise his or her rights as provided for in Section 32 of the AVCL. Furthermore, the amount of information demanded (on monthly income of the violator) is proportional to the purpose of personal data processing upon condition that the information may influence the type and amount of the applicable administrative penalty and it is provided by the person in order to realise his or her rights as provided for in Section 32 of the AVCL.

Consequently, the DSI established that the amount of the personal data on the number of dependants and monthly income demanded by the official of the

State Police when drawing up the notice on administrative traffic violation committed by a physical person, which is subject to administrative penalty pursuant to Article 149²⁸.2 of the Administrative Violations Code of Latvia, was not proportional to the purpose of personal data processing, considering that the person provided the information not in order to realise the right provided for in Section 32 of the AVCL but because the official had demanded that the said information be provided.

In the letter to the State Police, the Data State Inspection explained that in order to ensure the conformity of personal data processing to the Personal Data Processing Law, the following types of demanded information should be deleted from the notice form: 'Monthly income (LVL)' and 'Dependant persons', replacing them with the entry 'Other information', or the notice form should be supplemented with information on the conditions upon which the said information can be demanded (e.g. 'information entered if it is necessary in order to establish whether the application of the administrative penalty is not subject to any restriction', 'information included upon violator's demand').

On the right of the employer to look through e-mail correspondence of the employees

Pursuant to the e-mail letter received, the DSI provided its opinion on the right of the employer to look through e-mail correspondence of its employees under the following circumstances:

- the employer has developed the Information Security Policy, which is in force throughout the company and binding to all employees (the Policy discloses that the employer monitors and restricts the use of e-mail in accordance with the business needs of the company), but the employer has not introduced and explained the Policy to employees.
- there is not a formal written agreement on the monitoring of employee's e-mail neither in the employment agreement nor in a separate document.

The DSI provided the following explanation.

Pursuant to Section 2.4 of the Personal Data Processing Law, personal data processing means any operations performed with personal data and the processing may be performed if it conforms to the legal conditions specified in the Personal Data Processing Law (Sections 7,11,12,13.¹of the Personal Data Processing Law).

As regards the said situation, the legal basis for the personal data processing is Section 7.6 of the Personal Data Processing Law, which stipulates that 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 controller or of the third person to whom the personal data have been disclosed to.

The interpretation of the said section can be explained by using the following example: Pursuant to Section 61 of the Credit Institutions Law, credit institutions are obliged to guarantee the secrecy of the person, accounts, deposits and transactions of clients, while, in accordance with Sections 10.1.1 and 10.1.2 of the Personal Data Protection Law, the system controller, in order to protect the interests of the data subject (client of credit institution), has to ensure lawful and fair personal data processing and personal data may be processed only in accordance with the purpose intended and in the amount required therefor. Thus, the credit institution, by carrying out the monitoring of employee's e-mails with the purpose to control that personal data (of the credit institution clients) is not disclosed illegally to any third person, has not violated Article 7.6 of the Personal Data Protection Law . Furthermore, it has to be taken into account that the employer has provided its employees with means of communications (inter alia e-mail) to be used to perform their work tasks, therefore, the employer is entitled to control their use.

As regards the fact that the employer had not introduced nor explained the Information Security Policy to the employees. It was pointed out that, in

accordance with Article 8.1 of the Personal Data Protection Law, if personal data are obtained from a data subject, the system controller has the obligation to provide such information to the data subject unless the subject already holds such information:

1) the designation, or name and surname, and address of the system controller and personal data operator;

2) the intended purpose and basis for the personal data processing;

Thus, the processing of personal data was not compliant with the Personal Data Protection Law if the employee had not informed the data subject in accordance with the requirements under Article 8.1 of the Personal Data Protection Law.

As regards the way of certifying the fact that certain documents have been introduced to the employee, it was pointed out that it is not stipulated by the law. It was pointed out that since in accordance with Articles 10.1.1 and 10.1.2 of the Personal Data Protection Law the system controller, in order to protect the interests of data subjects, has to ensure lawful and fair personal data processing and personal data may be processed only in accordance with the purpose intended and to the extent required therefor, the system manager will have to prove that the information has been provided to the data subject to the extent specified in the Personal Data Protection Law.

Furthermore, it was pointed out that the procedure of personal data processing should be set out in the Information Security Policy (who is doing what; when and why it is done). For example, employees have to be informed on any restrictions imposed on their rights to use employer's means of communication, equipment and other property or information for personal needs (e.g. e-mail systems of banks are intended to be used only for work tasks) and informed also on the fact that it is being controlled (e.g. e-mail messages filtered, censored or blocked if they do not conform to the provisions on the use of employer's information systems and that the employer reserves the right to

monitor, archive and use incoming and outgoing e-mail messages of any employee).

On the right to disclose minutes of local government meetings to public

Pursuant to the request submitted, the DSI provided its explanation on disclosure of the local government council meeting minutes to public by submitting copies of the meeting minutes to the reading room collection of the local library and by publishing them on the website of the council.

Section 26 of the Law on Local Governments stipulates that meetings of local government councils shall be public and decisions and minutes of meetings of local government councils shall be publicly accessible so that the residents of and people working in the respective administrative territory and mass media journalists could access them free of charge.

Furthermore, Article 5.2.4 of the Information Freedom Law (whose purpose in accordance with Section 2 thereof is to ensure public access to the information held by state administration and local government institutions in order to perform the functions stipulated in regulatory acts) stipulates that information which concerns the private life of natural persons shall be deemed as restricted access information, and such information pursuant to Section 8 thereof is protected by law (inter alia the Personal Data Protection Law).

Consequently, council meeting minutes, if they conform to the term ‘information ‘ as specified in Section 1 of the Freedom of Information Law - information or compilations of information, in any technically possible form of fixation, storage or transfer, and if they contain personal data (which may be processed only if it conforms to the legal provisions on personal data processing as specified in the Personal Data Protection Law) may not be made publicly accessible (disclosing personal data) if there is no legal basis for such personal data processing.

It was pointed out, however, that it is necessary to ensure balance between the requirement under Section 26 of the Law on Local Governments to make

decisions of local government councils, orders of council chairpersons, and minutes of open meetings of local government councils (hereinafter – the documents) publicly accessible and the rights and freedoms (to personal data protection) of persons related to the documents.

The necessity to ensure the balance should not be interpreted as a necessity to remove all and any indirect personal identification data (in the meaning of the Personal Data Protection Law) from the documents. That would make it difficult to understand the documents and in many cases the documents would not be made publicly accessible at all since reading of the documents would create preconditions for the identification of the persons referred to therein. That would contradict to the principle of publicity of documents as stipulated by Section 26 of the Law on Local Governments. Therefore, the DSI pointed out that, considering the above-mentioned, local government councils should process the personal data in their decisions, chairperson's orders, and meeting minutes only to the extent that is required for the intended purpose. Furthermore, local governments, considering the specifics of dealing with certain issues and the types of personal data contained therein, in accordance with Article 26.3 of the Law on Local Government, should specify in the Regulation of the local government those matters that should be dealt with at closed meetings of the local government.

On the disclosure of the remuneration and bonuses of employees (other than civil servants and state officials) of the State Agency to public if the employee's position, name, surname, amount of remuneration and bonus is disclosed

Pursuant to the request, the DSI provided its explanation on the disclosure of the remuneration and bonuses of employees (other than civil servants and state officials) of the State Agency to public if the employee's position, name, surname, amount of remuneration and bonus is disclosed.

The DSI explained that the disclosure of personal data on the remuneration and bonuses and amounts thereof of the employees working with the Agency is permissible if any of the provisions referred to in Section 7 of the Personal Data Protection Law exists. For example, consent of the data subject has been received (in this case, the personal data processing conforms to Article 7.1 of the Personal Data Protection Law), the data processing is required in order for the system controller to exercise its obligations (in this case, the processing conforms to Article 7.3 of the Personal Data Protection Law) etc. Therefore, prior to disclosing any personal data of its employees to any third person, the Agency has to establish whether the third person has a legal basis pursuant to which it can demand any personal data of the employee and process them.

As it was pointed out, pursuant to Articles 10.1.1 and 10.1.2 of the Personal Data Protection Law, the system controller (the Agency), in order to protect the interests of data subjects, has to ensure lawful and fair personal data processing and personal data may be processed only in accordance with the purpose intended and to the extent required therefor.

On the processing of identity numbers in rent bills and public utilities bills made to flat owners

Pursuant to the received request, the DSI provided its explanation on the processing of identity numbers in rent bills and public utilities bills made to flat owners, in accordance with the Law on Value Added Tax

As regards the said case, the DSI explained that pursuant to Paragraph 2.4 of the Personal Data Processing Law personal data processing means any operations performed with personal data (including disclosure of personal data to third persons) and the processing may be performed if it conforms to the legal conditions specified in the Personal Data Processing Law (Sections 7,11,12,13.¹ of the Personal Data Processing Law). For example, personal data may be

processed if the data subject has given his/her consent to the processing thereof (Article 7.1 of the Personal Data Protection Law), if the data processing takes place pursuant to contractual relations of the data subject (Article 7.2 of the Personal Data Protection Law), if the data processing is required in order for the system manager to fulfil its obligations (Article 7.3 of the Personal Data Protection Law), and other cases.

In compliance with Article 12.1 of the Law on Business Activity, companies (business partnerships) have the obligation to perform accounting in accordance with the procedure set out in the relevant regulatory acts of the Republic of Latvia. The requirements on accounting are laid down in the Law on Accounting and Cabinet Regulations No. 585 of 21 October 2003 on Accounting and the Organisation thereof. In accordance with Article 7.1 of the Law on Accounting, the identity number has to be specified in justification documents under transactions with physical persons.

Therefore, if personal data of flat owners is processed (inter alia identity numbers) in accordance with the aforementioned regulatory acts, the personal data processing takes place in accordance with Article 7.3 and Article 13¹.2 of the Personal Data Protection Law.

On the right to specify the name of a medicament in the payment certification document

Pursuant to the received request, the DSI provided its explanation on the right of the Social Care Department to demand that the name of medication be specified in payment certification documents.

In accordance with Article 11.7 of the Personal Data Protection Law, sensitive personal data (personal data that discloses any information on personal health or sexual life) may be processed if it is required to render social assistance and if it is performed by the provider of social assistance.

Pursuant to Articles 10.1.1 and 10.1.2 of the Personal Data Protection Law, the system controller, in order to protect the interests of data subjects, has to ensure lawful and fair personal data processing and personal data may be processed only in accordance with the purpose intended and to the extent required therefor.

Considering the aforementioned, the DSI established that, in order to fulfil the objective specified in the Decision of City A, the Social Care Department may demand that the name of medicament be specified in payment certification documents. However, considering that the medicaments or groups thereof for which non-working pensioners and disabled persons of City A are entitled to receive allowances from the Social Care Department are not listed in the Decision of City A and it is stipulated in Paragraph 3.2 of the Decision of City A that only the name and surname and identity No. (not including the name of medicament) has to be specified in payment certification documents on purchased medicaments, the DSI pointed out that pursuant to Section 7 of the Personal Data Protection Law the Social Care Department, when developing the application form referred to in Paragraph 3.1 of the Decision, should include in it the provision that the person gives his/her consent to the specification of the name of medicament in the payment certification, thus receiving the consent of the person to the processing of the said data.

On the disclosure of information connected with road traffic safety and organisation on the Internet

Pursuant to the received request, the DSI provided its explanation on the fact whether mass media may disclose information connected with traffic safety and organisation on the Internet, including reports and photos from city roads (motorways, streets, boulevards, side-streets and similar territories, including carriageways, sidewalks, traffic islands, edges etc.) and other public territories

and which could contain peoples' faces, addresses and numbers of buildings, vehicle registration numbers, permits, passes, tickets etc.

As regards the said, the DSI explained that in compliance with Article 4.2 of the Personal Data Protection Law personal data processing means any actions performed with personal data.

Personal data may be processed if it conforms to the legal circumstances specified in the Personal Data Processing Law (Sections 7,11,12,13.¹ of the Personal Data Processing Law).

In accordance with Article 5.1 of the Personal Data Protection Law, Sections 7, 8, 9 and 11 of the Personal Data Protection Law are not applicable if personal data are processed for journalistic, artistic, or literary needs unless stipulated otherwise by law. Furthermore, in accordance with Articles 24.1 and 24.2 of the Law on Press and Other Mass Media, journalists have the right to collect information in any way that is not prohibited by the law and from any information source that is not prohibited by the law and to distribute such information.

Considering the above-mentioned, if the journalist has collected information in a way that is not prohibited by the law, then the personal data processing by publishing the above mentioned information in the electronic appendix of the newspaper conforms to the norms of the Personal Data Protection Law.

Furthermore, it was pointed out that it should be necessary to assess whether the extent of personal data processing is proportional to the purpose of the processing. Therefore, considering the right of persons to inviolability of private life as set forth in Article 5.2 of the Personal Data Protection Law, any personal identification information should be removed from pictures prior to publishing, if necessary.

On the personal data to be provided in declarations of state officials

Pursuant to the received request, the DSI provided its explanation on the types of personal data to be provided in declarations of state officials.

In respect of the right of state officials to provide identification data of third persons in declarations of state officials. The DSI pointed out that the said personal data processing may be performed upon legal basis – consent from the data subject (Article 7.1 of the Personal Data Protection Law).

In respect of the right of state officials not to provide identification data of third persons in declarations of state officials. The DSI pointed out that state officials have the right not to provide any personal data of third persons in the declarations if there is not a legal basis - consent from the data subject - for the processing thereof.

It was pointed out that not always officials held the personal data to be provided pursuant to the Law on the Prevention of Interest Conflicts in the Work of State Officials and Cabinet Regulations No. 478 of 22 October 2002 Procedure for the Completion, Submission, Registration and Keeping of Declarations of State Officials and the Submission of Registers of State Officials – e.g. identity numbers, addresses etc of parents and siblings, or the data held can be outdated or incorrect.

Considering the above-mentioned and that liability is stipulated in Article 166.27 of the Administrative Violations Code of Latvia for the provision of untruthful information in declarations of state officials, and that the request for the said information does not conform to Article 10.10 of the State Administration Structure Law, which stipulates that the state administration should be organised as possibly efficiently (so that the institutions that control declarations of state officials in accordance with their scope of competence, e.g. in accordance with Section 22 of the Resident Register Law, could be able to receive any information they need in order to exercise their functions from the personal data processing system ‘Resident Register’, which is maintained by the Department of Citizenship and Migration Affairs), the DSI considers that it

should be required to make amendments to the Law on the Prevention of Interest Conflicts in the Work of State Officials by deleting the norm that stipulates the obligation of state officials to provide personal data of third persons.

As regards the consent of the data subject and its form. The DSI explained that consent from third persons is required in order to include their data in the declarations of state officials. The Personal Data Protection Law does not stipulate that it is mandatory to make written consent.

On the processing of sensitive personal data of patients

Pursuant to the received request, the DSI provided its explanation on the processing of sensitive personal data of patients.

1. In respect of the right of medical institutions to disclose personal data of patients to insurance companies. Personal data that contains indications of the health state of the person are sensitive personal data in accordance with Article 2.8 of the Personal Data Protection Law, and such data may be processed if it conforms to the provisions under Section 11 of the Personal Data Protection Law.

The confidentiality of sensitive personal data is stipulated in Article 50.1 of the Medical Treatment Law (Information regarding the medical treatment of a patient, the diagnosis and prognosis of a disease (hereinafter – information regarding a patient), as well as information obtained by medical practitioners during the medical treatment process regarding the private life of a patient and his or her closest relatives, shall be confidential) and the persons who/which have the right to receive personal data of patients are specified in the articles below therein.

Considering the said, sensitive personal data may be provided to insurance companies and other companies if it conforms to any of the legal provisions as to personal data processing under Section 11 of the Personal Data Protection Law. For example, if the data subject has given written consent to the processing of his/her sensitive personal data (Article 11.1 of the Personal Data Protection Law).

Furthermore, it was pointed out that pursuant to Articles 10.1.1 and 10.1.2 of the Personal Data Protection Law the system controller, in order to protect the interests of data subjects, has to ensure lawful and fair personal data processing and personal data may be processed only in accordance with the purpose intended and to the extent required therefor.

2. In respect of the consent of patient. In accordance with Article 2.2 of the Personal Data Protection Law consent of a data subject to the processing of personal data is a freely, unmistakably expressed affirmation of the wishes of a data subject, by which the data subject allows his or her personal data to be processed according to information delivered by a system controller in compliance with Section 8 of Personal Data Protection Law. Pursuant to Article 11.1 of the Personal Data Protection Law, written consent of the data subject to the processing of his/her sensitive personal data is required. The written consent has to contain information that makes it possible to establish that it is a freely, unmistakably expressed affirmation of the wishes of a data subject, by which the data subject allows his or her sensitive personal data to be processed (delivered to third persons) for a certain purpose, and it also has to contain the information specified under Article 8.1 of the Personal Data Protection Law.

3. In respect of the documentation of the delivery of sensitive personal data. In accordance with Paragraph 4.5 of Cabinet Regulations No.40 of 30 January 2001 Obligatory Technical and Organizational Requirements for the Protection of Personal Data Processing Systems (issued pursuant to Section 26 of the Personal Data Protection Law) the system controller has to ensure that the following information is stored: the time of transfer of the personal data; the

person who transferred the personal data; the person who received the personal data; the personal data which were transferred.

On the right to publish (in newspapers) personal data of persons who have unsettled rent and public utilities payments.

Pursuant to the request received, the DSI provided its explanation on the right to publish (in newspapers) personal data of persons who have unsettled rent and public utilities payments.

Data of persons who have unsettled rent and public utilities payments may be published in local newspapers only if any of the legal conditions specified in the Personal Data Processing Law (Sections 7,11,12,13.¹ of the Personal Data Processing Law) is in place.

As regards the possible publication of the list of debtors in the newspaper *Latvijas Vēstnesis*, it was pointed out that in accordance with Article 2.4 of the Personal Data Protection Law personal data processing means any operations carried out regarding personal data, including data collection, registration, recording, storing, arrangement, transformation, utilisation, transfer, transmission and dissemination, blockage or erasure. Consequently, the publication of personal data in the official newspaper *Latvijas Vēstnesis* has to conform to the legal provisions regarding personal data processing as laid down in the Personal Data Protection Law. For example, Article 59.1 of the Civil Procedure Law stipulates that a defendant, whose place of residence is unknown or who cannot be found at their place of residence, shall be summoned to the court through publication in the newspaper *Latvijas Vēstnesis*; thus, in the said case, the personal data processing is permissible if the person is in the status of case participant (the person has been charged in accordance with the law) and the provisions under Article 59.1 of the Civil Procedure Law are in place.

On the accessibility to the children registration list (with registration queue number specified for every child) at a pre-school education establishment

Pursuant to the received request, the DSI carried out a control in relation to the children registration list (with registration queue number specified for every child) at Riga Pre-school Education Establishment No. 20 in connection with the provisions of the Procedure for the Enrolment of Children in Preschool Education Establishments and Establishments which Implement Preschool Education Programmes (hereinafter- the Regulations), which was approved by Riga City Council Education, Youth and Sports Department Director Order No. 106.

The Regulations set out the procedure whereby five-year and six-year old children are registered for the mandatory preparation for primary education. In accordance with Paragraph 8 of the Regulations, the register is accessible to parents, representatives of the Riga City Council Education, Youth and Sports Department, and representatives of other control institutions.

Pursuant to the said and considering the wording of the above-mentioned provision, the relevant legal provision may not be interpreted as an obligation of preschool education establishments to disclose, inter alia by placing the children registration list (with registration queue number specified for every child) in a public and accessible to everyone place at the preschool education establishment), any records of the register to third persons. The said conforms the provision under Articles 10.1.1 and 10.1.2 of the Personal Data Protection Law that the system controller, in order to protect the interests of data subjects, has to ensure lawful and fair personal data processing and personal data may be processed only in accordance with the purpose intended and to the extent required therefor.

As regards the right of parents to have access to the said children register, it was pointed out that, in order to ensure the right of parents to receive information on the movement of the queue (for enrolment of children in preschool education establishment) in relation to their child(ren), it is necessary to ensure a balance between the right of certain persons (parents) to receive information on the queue (for enrolment of children in preschool education

establishment) and the rights and freedoms of other persons included on the registration list. For example, in order to avoid any possible infringement of individual rights, the parents of a certain child should be provided only with information that is related to the movement of the queue (for enrolment of children in preschool education establishment) in relation to their child(ren) and that is included in the children register.

On the publication of the personal data obtained at open court hearings in newspapers

Pursuant to the received request, the DSI carried out a control in the case which had been instituted pursuant to a submission from a physical person with a request to carry out a control on the conformity of the actions of newspaper X – publishing an article, which contained personal data of person Y in connection with the judgement of the Riga Region Court in a blackmailing case - to the Personal Data Protection Law.

Pursuant to Paragraph 2.4 of the Personal Data Processing Law, personal data processing means any actions performed with personal data and the processing may be performed if it conforms to the legal conditions specified in the Personal Data Processing Law (Sections 7,11,12,13.¹of the Personal Data Processing Law). In accordance with Article 5.1 of the Personal Data Protection Law, Sections 7, 8, 9 and 11 of the Personal Data Protection Law are not applied if personal data are processed for journalistic, artistic, or literary needs and unless stipulated otherwise by law.

Furthermore, in accordance with Articles 24.1 and 24.2 of the Law on Press and Other Mass Media, journalists have the right to collect information in any way that is not prohibited by the law and from any information source that is not

prohibited by the law and to disclose such information. Consequently, unless provided for otherwise in regulatory acts, journalists on duty have the right to attend court hearings, record the information obtained at court hearings, and publish it.

In the control, the DSI established that the author of the article, journalist of the newspaper X, had obtained the information on person Y that was included in the said article during court hearings under the said case.

Pursuant to the said, the DSI did not establish any violations of the Personal Data Protection Law in the action of newspaper X - publication of information obtained at court hearings.

On the receipt of information from local government construction board in connection with the building permit and construction designs in relation to the reconstruction of certain houses

Pursuant to the received request, the DSI assessed the refusal of the Construction Board of Local Government X to provide information on the building permit and the construction design in relation to the reconstruction of the attic of the property at the address Riga, (...) Street, (...).

The Construction Board of the Local Government X refused to provide the information on the basis of Articles 5.2.4, 5.2.5, 5.2.6 of the Freedom of Information Law.

The DSI concluded that the issue of a building permit is the issue of a positive administrative act; consequently, as regards accessibility to information, the procedure had to be applied in accordance with the Administrative Procedure Law. Pursuant to Article 54.1 of the Administrative Procedure Law: If a request for information in connection with some administrative procedure is received from a private person, an institution shall provide the relevant information at its disposal, except in cases where this information is to be considered restricted access information in accordance with the law.

The status of restricted access information is stipulated under Section 5 of the Freedom of Information Law. The Construction Board of the Local Government X, in its refusal to the provision of information to person Y, had not provided a correct reference to the applicable norms of the Freedom of Information Law and had not interpreted correctly Article 5.2.6 of the Law; because information for official use is defined under Article 8.1 of the Freedom of Information Law and it applies to information connected with state security and cooperation of the state with official foreign authorities.

Pursuant to Section 8 of the Freedom of Information Law, any information on individual's private life is protected by the law. The Personal Data Protection Law stipulates the protection of private life with respect to personal data processing (Section 1). Pursuant to Article 7.5 of the Personal Data Protection Law, data may be processed if it is required to ensure that the public interests are complied with. Pursuant to the second sentence of Article 10.3 of the State Administration Structure Law - public interest shall include also proportionate observance of the rights and lawful interests of private individuals. Private individuals have the right to dispute administrative acts; therefore, information on the decision should be publicly accessible if the decision can restrict the rights and legal interests of the individual. Considering the said, the DSI established that the Construction Board of City X had violated Article 10.1 of the Freedom of Information Law in respect of the obligation to inform person Y on the building permit issued.

On the processing of personal data of minors on the Internet

On a website, which offers photo hosting services, there was a photo of a children (S) published. During the control, it was established that the personal data (photo) of the said minor had been published on the website by a registered user (N) of the website. The minor's mother (B) had objections against the publication of the photo and she filed a complaint to the DSI.

During the control, the DSI established that the person who filed the complaint and the person who, according to the information held by the DSI, published the photo were acquaintances (former friends), and the picture of S had been taken in the presence of B. According to the explanation of N, B had not had any objections against the taking of the picture. Considering the said, N had published the photo of S in the gallery created by N on the website, because she thought that she had the right to use the photo for personal needs.

B had not expressed any personal complaints on the publication of the picture to N nor provided any information on the origin of the photo to the DSI.

Having assessed the conformity of the said personal data processing to the Personal Data Protection Law, the DSI did not establish any violation of the Personal Data Protection Law committed by N; for, firstly, according to the materials of the case, B and N could have established between them such personal relationships under which the consent of B as the mother of S for the processing of the personal data of S could have been received, and, secondly, according to the explanation provided by N, the purpose of the publication of S's photo on the website had been the processing of personal data for artistic needs (the legal basis for personal data processing as stipulated by the Personal Data Protection Law).

However, as the DSI explained to B as the lawful custodian that she has the right to demand that N as the person who has processed the personal data of her minor daughter S and published her photo on the Internet terminates the processing of the personal data of S and deletes the photo from the said website.

On personal data processing in the context of the maritime law

The DSI received a submission from C with a request to assess the conformity of the personal data processing carried out by J.S., Head of the Seamen Register of the state stock company Latvian Maritime Administration, to the Personal Data Protection Law; J.S. had sent an e-mail message with

personal data of C and information characterising C as ship captain, from his official e-mail address to a number of seamen employment agencies.

In the control the following was established.

The state stock company Latvian Maritime Administration as a maritime administration body is responsible for the implementation of the requirements of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers of 7 July 1978, inter alia in relation to the assessment of competences of seamen, issuing of internationally recognised competence certificates to seamen working on ships, keeping of a register of all and any data related to the competence of seamen, data processing and information exchange (Provision I/9, Article 4; provision I/14, Article 1.3, Code B-I/19, Articles 14,15, and 16). Whereas the Seamen register of the Latvian Maritime Administration, pursuant to the relevant regulatory acts, monitors the seafaring and seamen employment agencies of Latvia. Regulation I/14 of the Convention sets out the responsibility of the Member States to ensure that the provisions of the Convention in relation to maritime safety are complied with in the employment of seamen and the staffing of ship teams. Inter alia, pursuant to Regulation I/14, Article 1.3, the Member States have to ensure that seamen employment agencies hold data on the seamen who seek employment.

The Seamen Register of the Latvian Maritime Administration had received information on the unconformity of C to the position of a captain from a number of seamen employment agencies, which stated the reason – excessive use of alcohol, due to which C has endangered maritime safety, maritime traffic, and peoples' lives. Furthermore, The Seamen Register of the Latvian Maritime Administration had received a report from the Swedish Maritime Agency on an accident with the ship S near the coast of Sweden and which C had caused being under the influence of alcohol; in connection with the said accident the Maritime Agency of St. Vincent and Grenadines, under the flag of which the ship was, had cancelled the endorsement of the competence certificate and prohibited C to take any position on ships of the country, and the Latvian Maritime

Administration had been notified on the said fact. Consequently, the Seamen Register of the Latvian Maritime Administration, by providing information on C to the seamen employment agencies, fulfilled its obligations under international treaties binding to the Republic of Latvia and acted in international public interests (the purpose of personal data processing - to facilitate a more responsible attitude of seamen employment services towards staffing of ship teams; the legal basis – Article 7.5 of the Personal Data Protection Law [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 a system controller or transmitted to a third person]).

Furthermore, the Ministry of Transport and Communications, as the authority which implements the general control of the State over maritime affairs, inter alia state supervision and control over the implementation and administration of the state's functions that are commissioned to state administration institutions that are under the subordination of the Ministry and companies managed by the Ministry, within the scope of its competence provided its explanation on the legal basis and purpose for the processing of the personal data of C. In the explanation, pursuant to Regulation I/5, Article 1 of the Convention (Each Party shall establish processes and procedures for the impartial investigation of any reported incompetence, act or omission, that may pose a direct threat to safety of life or property at sea or to the marine environment, by the holders of certificates or endorsements issued by that Party in connection with their performance of duties related to their certificates and for the withdrawal, suspension and cancellation of such certificates for such cause and for the prevention of fraud); Regulation I/9, Article 4.2 of the Convention (Each Party undertakes to make available information on the status of such certificates, endorsements and dispensations to other Parties and companies which request verification of the authenticity and validity of certificates produced to them by seafarers seeking recognition of their certificates under

regulation I/10 or employment on board ship), Regulation I/14, Article 1.3 of the Convention (Each Administration shall, in accordance with the provisions of section A-I/14, hold companies responsible for the assignment of seafarers for service in their ships in accordance with the provisions of the present Convention, and shall require every such company to ensure that: documentation and data relevant to all seafarers employed on its ships are maintained and readily accessible, and include, without being limited to, documentation and data on their experience, training, medical fitness and competency in assigned duties), the Maritime Department of the Ministry of Transport and Communications pointed out that there have been reasonable doubts to suspect the ability of C to perform the tasks of a captain of ship and there has been a considerable risk that the employment of C in the said status might endanger other people's health and lives, maritime traffic safety, as well as result in loss of material and ecological character. Therefore, considering also Article 10.3 of the State Administration Structure Law (*State administration shall act in the public interest. Public interest shall include also proportionate observance of the rights and lawful interests of private individuals.*), the Maritime Department of the Ministry of Transport and Communications established that the Seamen Register of the Latvian Maritime Administration had justifiably applied Article 7.5 of the Personal Data Protection Law in relation to the processing of the personal data of C and the disclosure of the information characterising C as a ship captain to seamen employment agencies.

Considering the aforementioned and having assessed the conformity of the said personal data processing to the Personal Data Protection Law and other regulatory acts, the DSI concluded the following.

The Seamen Register of the Latvian Maritime Administration, in monitoring seamen employment agencies, has the right to perform personal data processing within the scope of its competence in relation to the professional activities of seamen (inter alia in connection with law violations committed by seamen) in accordance with Provision I/5, Article 1 of the Convention. Pursuant

to the said and in accordance with the general legal principles, Section 7 of the Personal Data Protection Law, Sections 13 and 15 of the Administrative Procedure Code, Article 10.3 of the State Administration Structure Law, and Section 13 of the Law on International Treaties, the DSI, in relation to the action of the Seamen Register of the Latvian Maritime Administration - the disclosure of the information characterising C as a captain of ship to seamen employment agencies – was not a violation of the Personal Data Protection Law.

However, considering that the regulatory acts of the Republic of Latvia do not specify the procedure whereby reports on the lack of competence of competence certificate holders (seamen) issued by a Member State are examined, as regards the right of the Seamen Register of the Latvian Maritime Administration to process the personal data of the seamen registered in the personal data processing system controlled by it by transferring the said data to seamen employment agencies in connection with law violations committed by the said seamen, the DSI pointed out that the Maritime Department of the Ministry of Transport and Communications should make amendments to the relevant regulatory acts in order to ensure that the procedure of personal data processing to be applied for impartial investigation of any reported incompetency, act or omission, that may pose a direct threat to safety of life or property at sea or to the marine environment, by the holders of certificates or endorsements issued by that Party in connection with their performance of duties related to their certificates is set out.

On the right of the cooperative society to publicise a court decision on a member of the cooperative society

J.S, Board Chairman of Non-profit Garage Owners Cooperative Society V (NGOCS V), had put on the message board of NGOCS V (situated on the outside of the building) the judgement of the Rēzekne City Court in Case No. XXXXXX – NGOCS V (a claim against D.P. on the collection of loss). In the

control, it was established that D.P. had been a former Chairman of NGOCS V (now- a member of NGOCS V) and the claim had been made in connection with disbursements made by D.P. as the Chairman and Technical Manager of Electrical Equipment of NGOCS V.

As regards the said personal data processing, J.S. explained that, considering the request of the members of NGOCS V, the said personal data processing had been performed in order to inform the members of NGOCS V and that it had been done pursuant to the decision of the General Meeting and the Board of NGOCS V. During the control, the decision of the General Meeting of NGOCS V, which stipulated the publicising of the procedural documents (in relation to D.S.) connected with the proceedings, was not submitted to the DSI.

D.P. as a member of NGOCS V had not had provided his consent to the said personal data processing and he asked the DSI to apply an administrative penalty to NGOCS V.

In accordance with Paragraph 5.8 of the Articles of Association of NGOCS V, its members have the right to receive information from the Society on any issue connected with its operation. However, since the said Rēzekne City Court Judgement in Case No. XXXXXXX had been posted on the message board of NGOCS V, which is located on the outside of the building, the personal data of D.P. could have been obtained not only by members of NGOCS V but also other persons not to be consider as lawful recipients of the said information as stipulated by the law.

Pursuant to the established facts, it was concluded that NGOCS V had performed the personal data processing by violating the legal provisions of personal data processing under Section 7 of the Personal Data Protection Law (illegal personal data processing), which, pursuant to Section 204⁷ of the Administrative Violations Code of Latvia, is subject to administrative liability (illegal personal data processing). The DSI made a decision to apply a fine of LVL 120 (one hundred and twenty lats) to NGOCS V.

On data quality in connection with the right of an insurance company to include personal data in the database controlled by it

The DSI, on the basis of the complaint of G.I. and other materials of the case, established that J.L., an official of the insurance stock company (ISC) had permitted the personal data processing of G.I. without any legal basis thereof. G.I., Manager of Petrol Station No. 7 of the Limited Liability Company V, was invited to and took part in the training on the distribution of third party liability insurance of motor vehicle owners policies of the Insurance Company B (hereinafter-the insurance policies). In the agreement concluded between SIA Viada and the Insurance Company it was stipulated that managers of petrol stations would distribute the insurance policies. A written agreement between the Insurance Company and G.I. on the distribution of insurance policies was not concluded due to the fact that the legal labour relationships between G.I. and SIA Viada were terminated. Furthermore, J.L., Project Manager of the Insurance Company, had not controlled whether the relevant agreement had been concluded with G.I.; in the result, the employees of the Insurance Company entered the personal data of G.I. (name and surname) in Polvadis, the policy making system of the Insurance Company, as the data of an agent of the Insurance Company.

In accordance with the materials of the case, the DSI established that the personal data of G.I. (name and surname) had been included in ten insurance policies – TS standard agreements No. 874... - 874... without any legal basis therefor. The validity period of the insurance policies was specified, and none of them has been cancelled. At the time of the adoption of the decision of the DSI, two policies were still in force and eight of them had expired.

J.L., who was responsible for the said entering of personal data and the control of the correctness of the data in Polvadis, the policy making system, during the investigation admitted the administrative violation committed, i.e. illegal personal data processing, which took place as illegal personal data

processing without any legal basis therefore and as the entering of the personal data of G.I. in the personal data processing system Polvadis, in the result of which the data were included on the insurance policies as the data of a representative of the Insurance Company.

In accordance with Articles 7.1 and 7.2 of the Personal Data Protection Law, personal data processing is permitted only if not prescribed otherwise by law: the data subject has given his or her consent; the personal data processing results from contractual obligations of the data subject or, observing request of the data subject, the data processing is necessary for the conclusion of the corresponding contract. The liability for the violation of the said provisions of the law is stipulated under Article 204⁷.1 of the Administrative Violations Code of Latvia (for illegal personal data processing).

In this case, the DSI adopted the decision to apply an administrative penalty – a written warning – to J.L., Project Manager of the Insurance Company.

On the right of data subjects to receive medical documentation

V.T. turned to the DSI in relation with the fact that the Medical Care and Work Ability Expertise Quality Control Inspection (Latvian acronym – MADEKKI) had refused to provide her with copies of certain documents held by MADEKKI in relation to a case handled by MADEKKI pursuant to a submission from V.T (she filed a complaint to MADEKKI in relation to paid dental treatment, which had been unqualified).

The DSI as the authority that monitors personal data protection and the freedom of information in Latvia was asked to assess the refusal of MADEKKI to provide V.T. with copies of the medical (ambulatory) cards requested by her. V.T. is aware of Cabinet Regulations No. 275 of 3 August 2005 Procedure for the Disclosure of Information Held by State Administration and Local Government Institutions, which stipulate that institutions may refuse to provide information if the author of the information is another institution, organisation or

company; however, she pointed out that MADEKKI had in past provided her with documents (copies) the authors of which have been other institutions. Considering the said, the DSI was asked to provide a justification for the refusal of MADEKKI to provide V.T. with copies of medical (ambulatory) cards held by various medical institutions, considering that they are an integral part of the file and provide her, as a data subject, with information on her health condition.

In connection with the said, it has to be pointed out that the totality of certain actions that the DSI has the right to carry out in relation to the freedom of information in the regulatory acts, as the Freedom of Information Law specifies only a general regulation of the sphere (The DSI monitors the compliance with the Freedom of Information Law in accordance with the procedure specified in the regulatory acts). Furthermore, Section 61 of the Administrative Procedure Law (stipulates the right of participants of administrative proceedings to get acquainted with the matter and express his or her opinion at any stage of the proceedings) could not be applied, because at the time of filing the submission to MADEKKI the person was not a participant of the administrative proceedings anymore. Consequently, considering the said and the fact that MADEKKI as an institution that is not the author of the requested medical documents had the right to refuse to issue copies of the medical documents, in this case the DSI recommended the person to use the right to request the information from the respective medical institution, which treats (treated) her health.

6. Participation of the Data State Inspection in Proceedings

In 2005, four decisions of the DSI in administrative violation cases were appealed. Three decisions were made in relation to data processing in video surveillance and one decision was made in relation to illegal obtaining of data from a personal data processing system. None of the decisions of the DSI had been cancelled or passed for further examination by the court in 2005.

7. Audit and Auditors of Personal Data Processing

In accordance with Article 29.3 of the Personal Data Protection Law, one of the duties of the DSI is to accredit persons wishing to perform system auditing of personal data processing systems of government and local government institutions in accordance with the procedure established by the Cabinet of Ministers. Cabinet Regulations No. 25 Procedure for the accreditation of persons who wish to perform system auditing of data processing systems of government and local government institutions were adopted on 13 January 2004; the Regulations set out the procedure whereby the DSI accredits persons who wish to carry out system auditing of data processing systems of government and local government institutions.

Once a quarter, the DSI publishes in the official newspaper Latvijas Vēstnesis and the website of the DSI the information on the accreditation certificates issued to system auditors and cancelled, suspended and renewed accreditation certificates, renewal and invalidation thereof. The DSI accredits physical persons who conform to the criteria specified in the regulatory acts. In the Regulations, individual specific requirements for internal and external auditors of personal data processing systems are determined. System auditors are accredited for a period of three years.

In accordance with Cabinet Regulations No. 25 Procedure for the accreditation of persons who wish to perform system auditing of data processing systems of government and local government institutions, 14 internal system auditors and 5 external system auditors were accredited in 2005. In total, 60 internal personal data auditors and 13 external personal data auditors have been accredited by the DSI.

The DSI has prepared the instructions on the audit of personal data processing systems; the Instructions are publicly accessible on the website of the DSI: http://www.dvi.gov.lv/fpda/files/fpda_audita_rokasgramata.pdf. The Instructions were developed to assist auditors of personal data processing to carry out auditing and to acquaint any interested person with the purposes, methods, and procedures of the audits, and to provide general recommendations on auditing. The Instructions has a number of annexes – forms containing

assessment questions on every personal data protection principle as specified in the Personal Data Protection Law, and the forms can be used in practice for auditing.

According to Article 26.2 of the Personal Data Protection Law, each government and local government institutions shall submit annually to the State Data Inspection an opinion on internal audit of personal data processing systems (including system risk analysis, as well) and a report on measures taken in the sphere of information security.

Cabinet Regulations No. 40, which were issued pursuant to Section 26 of the Personal Data Protection Law, contain a norm under Paragraph 6 that system controllers shall carry out the internal personal data processing system audit annually and prepare a report on the measures taken in the sphere of information security.

Opinions on internal audits have been submitted by 48 government institutions; 19 of those government institutions that employ accredited auditors have submitted the said reports. 13 of the accredited internal auditors have submitted the said opinions, while 25 of the non-accredited auditors have submitted opinions on internal audit of personal data processing, which proves the necessity also in future to support the accreditation of auditors and the facilitation of the cooperation with officials of internal audit units of state administration institutions.

The analysis of the submitted opinions on internal audit is carried out on a regular basis and the common detected failures as to data protection at institutions are registered. By comparing the reports, it is possible to follow the establishment of the personal data protection system in government institutions. A progress can be seen – if in the first year failings had been detected in personal data protection, then in the next year they have been rectified.

8. Public Information and Social Activities

A successful communication with public, professional associations and non-governmental organizations is one of the main basic principles of a developed and active state administration system. Involvement of a society in the policy making process ensures a successful fulfilment of tasks and a stable long-term development. Targeted public information about work, recent developments and future plans of state administration is required for the cooperation of the society and the government. Thus, by understanding the ongoing processes, each member of the society can make his own opinion and participate in the making of political decisions both as an individual and as part of the society.

While informing the society, the Data State Inspection (SDI) has identified two main target audiences – a data subject and a personal data processing system controller. During the reporting period the society was regularly informed about the activities, aims and tasks of SDI. Particular attention was paid to the latest developments related to the application of legal provisions on privacy protection and the latest trends as to data protection in the European Union.

Public information is provided through the internet web site of the Inspection - www.dvi.gov.lv. The information on the web site is updated every week. Its target audience are individuals, whose privacy rights are or could be infringed, personal data processing system controllers etc.

Active interest of students about issues of personal data protection was observed in 2005, thus it is evident that the questions of privacy and personal data protection are analysed also in academic circles. Six students had the possibility to undergo practical training related to their studies at the DSI.

In connection with public information, the work with mass media is also important, which in comparison to previous years was actively carried out in 2005 on the basis of the Communication Strategy of the SDI, which provides

regular contacts with mass media, public information campaigns and also the improvement of the internal communication in order to raise the capacity of employees.

Public activities

Public opinion is important not only in relation to the decision making process, but also in developing the future development plan for the institution, including in it solutions of problems topical for the society. Therefore, a public opinion poll about personal data protection was carried out in 2005. 1007, 18 to 74 years old permanent residents of the Republic of Latvia were involved in this poll according to the principle of random stratification.

More than a half (52.9%) of the respondents considers that personal data that are held by various institutions are partly protected against the possibility to be obtained by some unauthorized person or institution. Only 7.2% of the respondents expressed the opinion that this information is well and safe protected.

10% - 20% of the respondents have had various problem situations related to data processing and protection.

19.5% of the respondents have experienced situations where mistakes had been made in the processing of their data that could incur financial or moral damage. Compared to the results of the study in 2003, the number of such respondents has slightly increased (from 14.5% to 19.5%).

13.5% of the respondents have experienced situations where the extent request of personal data was larger than was necessary. In comparison with the results of the study in 2003, the number of such respondents has doubled (from 6.4% to 13.5%).

13.4% of the respondents have experienced situations where their data were obtained by a third party and had been used to gain a material benefit or they had incurred some loss. In comparison with the results of the study in 2003,

the number of such respondents has decreased in this year (from 20.7% to 13.4%).

11.7% of the respondents have experienced situations where data of particular value were obtained by a third party. In comparison with the results of the study in 2003, the number of such respondents has slightly increased (from 7.9% to 11.7%).

Almost every third respondent (29.5%) has heard about the SDI. This number is higher than that under the study carried out in 2003 (23.3%).

22.9% of the respondents have tried to get information about themselves from an institution or company. Most of them (66.2%) have not experienced situations that the institutions or companies which processed their data would refuse to provide the said information. 32.5% of the respondents who have tried to receive information about themselves have had a negative experience (institutions or enterprises refused to give the information). The data obtained from the study show that the information about issues of personal data protection is topical for both the society and employees of state administration bodies; therefore, the public information work will be continued also in 2006, inter alia the preparation of informative materials.

9. International Activities of the Data State Inspectorate

As to the international relations of the DSI, the year 2005 brought about a kind of a challenge, which was due to the fact that Latvia accessed to the European Union in May, 2004; following the accession, a wider range of possibilities to take active part in solving data protection issues not only on the national level but also on the transnational level. Employees of the DSI took part in working groups, conferences, seminars on the EU level and on the international level in order to facilitate the implementation of the best data protection principles in Latvia.

As regards the activities within the European Union, the priorities set by the European Commission had to be considered. One of the most current issues set was the data protection within the framework of the third pillar and the transfer of personal data to third countries.

Article 29 Working Party under Directive 95/46/EC

The Article 29 Working Party under Directive 95/46/EC was established pursuant to Article 29 of the Directive on the protection of individuals with regard to the processing of personal data. The Working Party has advisory status and acts independently. The Working Party is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party is designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same applies to the authorities established for Community institutions and bodies. Latvia is represented at the Working Party by the Director of the DSI.

The Working Party takes decisions by a simple majority of the representatives of the supervisory authorities. The Article 29 Working Party considers items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request

The Article 29 Working Party under Directive 95/46/EC is an advisory body, which is represented by heads (or persons authorised by them) of personal data supervisory institutions of the Member States of the European Union together with representatives of the European Commission.

At the Working Party, Member States provide regular reports on every country individually in relation to the administrative practice, examination of practical issues, most significant court proceedings, cooperation with private companies, cooperation with other institutions both at the national and the international levels.

Tasks of the Working group of Article 29 under Directive 95/46/EC:

- examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
- give the Commission an opinion on the level of protection in the Community and in third countries;
- advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
- give an opinion on codes of professional conduct of the Community level.

If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall

inform the European Commission accordingly. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31 of Directive 95/46/EC. The European Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. The European Commission shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the European Commission, the European Parliament and the Council. The report shall be made public. In 2005, also Latvia as a full-fledged Member State of the European Union drew up an informative report.

As from May 1, 2004, Latvia became a full-fledged member of the Working Party and it takes part in the preparation of recommendations and decisions and the decision-taking process. Following the extension of the European Union, when Latvia obtained the status of a full-fledged member of the Working Party, its chairman called on Latvia and other countries to take more active participation in the work of the Working Party and the subgroups established by it, in that way obtaining experience and facilitating the information exchange with colleagues from other EU Member States. Therefore, the DSI will consider the issue on possible participation in some of the subgroups in 2006.

The recommendations and guidelines developed by the Article 29 Working Party can be used in practice not only by personal data supervisory institutions of the EU but also by data controllers which operate within the EU. The said guidelines help in achieving more harmonised implementation of Directive 95/46/EC within the European Union.

In 2005, the Working Party developed the guidelines on the use of biometric data in passports, the transfer of data to third countries, and the use of location data in the service provision. The guidelines are published on the website of the European Commission (http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm).

The most important issues dealt with by the Article 29 Working Party in 2005:

- simplification of the registration procedure of personal data registration systems;
- the Personal Data Protection Law under the framework of Pillar III;
- biometry and EU passports;
- transfer of personal data of passengers to the USA, Canada, Australia;
- the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism retention.
 - Safe Harbour Privacy Principles;
 - data protection and RFID technologies;
 - data protection and rules on internal whistle blowing schemes;
 - Information System *Visa*;
 - Schengen Information System.

For further information, visit the website of the European Union: http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

Since Latvia is a Member State of the European Union, the work on various issues is carried out both on the national and the transnational levels. One example is the issue on data protection within the third pillar, when the work was carried out within the 29 Article Working Party under Directive 95/46/EC and also in Latvia – developing and approving the national position with the

Ministry of the Interior. The issue of the application of data protection principles to the police sector has become very topical in the context of terrorism combating. Directive 95/46/EC is applicable to the first pillar, which does not cover the police sector but the commercial sector, free movement of goods, services and persons.

Article 31 Committee under Directive 95/46/EC

In the sphere of personal data protection, the European Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the European Commission. The representative of the European Commission shall submit to the Article 31 Committee a draft of the measures to be taken in relation to the documents developed by the Article 29 Working Party. The committee shall deliver its opinion on the said draft. As from 1 May 2004, when Latvia became a full-fledged member of the Committee, also representatives from the DSI have been taking part in the Committee.

To make personal data protection topical, a lot depends also on the presiding Member State of the European Union. In 2005, Luxembourg and the United Kingdom were the presiding Member States, and their personal data protection supervisory authorities are actively engaged in the said matters on the EU level. One of the most topical issues in 2005, which was commenced already in 2004, was data protection within the framework of Pillar III and the possible amendments in connection with Directive 95/46/EC, and the improvement of cooperation among data protection institutions.

As from spring 2006, Latvia will be represented in the Article 31 Committee by representatives from the Ministry of Justice.

Spring Conference of European Data Protection Authorities (Krakow, Poland)

The Spring Conference is to be regarded as the most significant annual event of the European Data protection Commissioners, which is attended also by representatives from outside the European Union. The first Spring Conference took place in 1991 in Hague. In 1993, the Conference took place in Paris, when the decision to organise the conference every year in spring was taken. On 24-26 April 2005 the Spring Conference of European Data Protection Authorities was organised by the Polish Data Protection Authority.

The said conferences are usually devoted to various personal data protection aspects in Europe, therefore its attendants not only deal with issues on the application of EU data protection norms in practice but also on the data protection practices in every individual country. Since 2005 was the 10th anniversary of Directive 95/46/EC, the Conference assessed generally the provisions of the Directive and application thereof in practice, considering the growing risks in respect of individual rights to privacy and data protection. The subject of the Conference was the 10th anniversary of adopting a resolution of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on free movement of such data.

The conference focused special attention to the following matters:

- the influence of Directive 95/46/EC on the level of personal data protection in the European union and third countries;
- Assessment of Directive 95/46/EC and the implementation of the provisions thereof in practice;
- - personal data protection within the framework of Pillar III;
- New legal instruments that allow transferring data to third countries;
- Education of the society on data protection;
- Use of the right (receipt of their data) of data subjects in practice.

The Conference adopted the Krakow Declaration approving the plan of the EC to develop a new legal framework for data protection in the third pillar and the

establishment of a working group whose task is to continue the work in relation to the personal data protection in the work of law enforcement institution and in particular in relation to the simplification of the information exchange procedure among law enforcement institutions of Member States.

The Spring Conference 2006 will be organised by the Hungarian Data Protection Authority; it is considered to be a significant factor for the integration of the new Member States for common work – the improvement of data protection and the facilitation of compliance with human rights.

7th Meeting of the Central and Eastern European Data Protection Commissioners (Smolenice, Slovakia)

In 2001, the 1st Meeting of the Central and Eastern European Data Protection Commissioners took place in Warsaw, Poland. The objective of the Meeting was to exchange with the most current information as to personal data protection among the Central and Eastern European data protection authorities and to find practical solutions for various personal data protection problems. The most important aspect of the said meetings is to solve problems that are characteristic of the new Member States and the candidate countries in order to ensure an adequate level of personal data protection.

Since the extension of the EU on 1 May 2004, Commissioners of data protection authorities decided to continue the cooperation and organise annual meetings, the purpose being:

- to assist the Central and Eastern European data protection authorities in solving practical issues;
- to find practical solutions for the implementation of Directive 95/46/EC.

On 23-24 May 2005 the 7th Meeting of the Central and Eastern European Data Protection Commissioners took place in Smolenice (Slovakia). The topics of the 7th CEEC Meeting were: processing biometrics data (new technologies in

practice), administrative and judicial proceedings and disclosure of information, scope of the use of Personal Identification Number, application of information system security standards in personal data processing and personal data processing for statistical purposes, and personal data protection in medical treatment.

Pursuant to the decision of the 6th Meeting of the Central and Eastern European Data Protection Commissioners, took place in Riga in May 2004 and to provide a summary on the work in previous years, the Central and Eastern European Data Protection Commissioners signed the Declaration on future cooperation and the readiness to share experience and provide assistance to the new EU candidate countries was expressed.

The Declaration stressed that particular efforts should be dedicated to improving and increasing the awareness of individuals and institutions of the principles, rights and obligations concerning personal data protection. The Declaration expressed support to the proposal of the European Council to proclaim the 28th of January the European Data Protection Day; The Declaration stated that special attention should be paid to youth by initiating projects related to data protection. The Declaration was signed by heads of the data protection authorities of Latvia, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Lithuania, Poland and Slovakia.

In 2006, the CEEC meeting will be organised by the Personal Data Protection Commission of Bulgaria, and it is planned to invite to it new representatives from other Eastern Europe countries.

Europol Joint Supervisory Body

The establishment of Europol was approved on 7 February 1992 by the Maastricht Agreement. Europol, with the Headquarters in Hague, the Netherlands, commenced restricted operations in combating drugs on January 3,

1994 as the Europol Drugs Unit (EDU). Gradually, other significant spheres of crime were added to its scope of competence. Since January 1, 2002, the range of tasks of Europol has been expanded in order to combat serious forms of international crime as set out in the Europol Convention and the Annex thereto (unlawful drug trafficking, unlawful immigration networks, illegal trade in vehicles, trafficking in people, including child pornography, forgery of money (euro) and other means of payment, money laundry).

The cooperation as to solving the said issues includes also the information exchange with personal data and sensitive personal data; therefore, the Europol Convention included provisions on personal data protection. To ensure that the personal data protection principles are complied with in the work of Europol, the Joint Supervisory Body (an independent body) was established pursuant to Article 24 of the Europol convention.

The Joint Supervisory Body of Europol controls the use and contents of all the personal data held by Europol, and it has the right to carry out audits within Europol. Latvia became a full-fledged member of this authority in September 2004, and it is represented by the Director of the DSI. Meetings of the Joint Supervisory Body are held as minimum four times a year.

In 2005, a report on the measures required to ensure personal data protection for the needs of Europol was prepared, and it was worked on the development of a mechanism for the supervision over data processing in Latvia within the framework of the Europol Convention.

For further information, visit the website of the Joint Supervisory Body: <http://europoljsb.ue.eu.int>.

Joint Supervisory Body for the Customs Information System

The Joint Supervisory Body for the Customs Information System is an independent authority, which supervises the Customs Information System of the European Union.

The objective of the Customs Information System is to facilitate and expedite the information exchange among cooperation authorities. The system contains a central database, access to which is given only to the EU Member States and the European Commission. The database contains only data (including personal) that are required for the implementation of customs-related regulations. The personal data that can be stored in this system for the said purpose have been clearly specified. The principles of personal data protection are binding to the said storage and processing of data.

National data protection authorities of Member States have the supervision over the Customs Information System ensuring that the use and processing of personal data entered therein would not infringe the right of the data subjects to personal data protection. To fulfil this task, national supervisory bodies of the CIS cooperate. In 2003, the Joint Supervisory Body for the Customs Information System invited the DSI to take part in the status of observer at its meetings.

In 2005, the DSI prepared an informative report on the required measures in order to ensure the personal data protection of the data used in the Customs Information Systems.

Pursuant to Article 2 of the Convention on the use of information technology for customs purposes, drawn up on the basis of Article K.3 of the Treaty on European Union, EU Member States develop and maintain a joint information system for the purposes of customs (hereinafter – the Customs Information System). Latvia, in accordance with Section 1 of the Law on the Convention on the use of information technology for customs purposes, drawn up on the basis of Article K.3 of the Treaty on European Union, Agreement on provisional application between certain Member States of the European Union , PROTOCOL drawn up on the basis of Article K.3 of the Treaty on European Union, on the interpretation, by way of preliminary rulings, by the Court of Justice of the European Communities of the Convention, Declaration on Simultaneous adoption of the Convention and the Protocol made pursuant to Article 2 of the Protocol (hereinafter – the Law on the Convention), has

accessed to and approved the Convention on the use of information technology for customs purposes, drawn up on the basis of Article K.3 of the Treaty on European Union (hereinafter –the Convention).

Section 3 of the Law on the Convention stipulates that the supervision of personal data pursuant to Article 17 of the Convention is carried out by the DSI. In Latvia, the legal protection of personal data is connected with the ratification of the 108th Convention on 5 April 2001 and the implementation of the basic principles of the EU Directive in the Personal Data Protection Law, which was adopted on 23 March 2000. To ensure complete compliance with the requirements of the European Union under Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the Parliament adopted the Law on the Amendments to the Personal Data Protection Law on October 24, 2002. Thus, the Personal Data Protection Law was aligned with the personal data protection principles of the European Union and the Europol.

To supervise the compliance with the personal data protection principles in the Customs Information System, in accordance with the Convention correspondence and a number of meetings was organised with representatives of the State Revenue Service.

In accordance with Article 17, each Member State shall designate a national supervisory authority or authorities responsible for personal data protection to carry out independent supervision and ensure that the processing and use of data held in the Customs Information System do not violate the rights of the person concerned.

For the DSI to be able to exercise its supervisory functions in the Customs Information System, the DSI, in accordance with Article 17.1 of the Convention, has to have access to the Customs Information System and the description of the software used in the Customs Information System.

Pursuant to Article 17.2 of the Convention, checks shall be carried out by the DSI in close coordination with that Member State's national supervisory authority.

The DSI, in cooperation with the State Revenue Service, has to develop the instructions and methodology to be used by the structural units in personal data processing cases. The instructions and methodology are to be developed in compliance with the norms of the Convention and the Personal Data Protection Law.

In the implementation of the required measures to ensure personal data protection in the Customs Information System, the main problems that the DSI faced were – a national supervisory body for the Customs Information System has not been established yet and the existing capacity of the DSI might be insufficient to carry out quality checks of personal data processing in the Customs Information System.

Joint Supervisory Body for the Schengen Information System

The Joint Supervisory Body for the Schengen Information System is an independent body, with its Headquarters in Brussels, Belgium, and it is composed of representatives of the national data protection authorities as stipulated in the Convention on the Implementation of the Schengen Treaty (hereinafter – the Schengen Convention).

The Joint Supervisory Body has dealt with many significant matters, and in some cases a decision has been taken, as stipulated by the Schengen Convention – to stress the required information in the management of the Schengen Information System and/or point out shortcomings.

The Joint Supervisory Body has carried out a number of control measures in the central technical support unit of the SIS in Strasbourg, and it has pointed

out that the system work is appropriate, at the same time a number of problems were pointed out.

In 2003, the Joint Supervisory Body for the Schengen Information System invited the DSI to take part in the status of observer at its meetings until the ratification of the Schengen Convention.

The SIS has existed as a mechanism that provided information to the member states of the Schengen Convention. The information is related to the movement of persons and goods; also the information required to ensure the cooperation of police authorities was provided to serve the purposes set out in the Schengen Convention following the cancellation of borders. As the European Union has expanded, the development of a new Schengen Information System is being discussed.

International Working Group on Data Protection in Telecommunications (Berlin, Germany)

The International Working Group on Data Protection in Telecommunications was established upon the initiative of Data Protection Commissioners with the purpose to improve the data protection in telecommunications and mass media. The Working Group holds its meetings twice a year, and they are dealing with IT matters in connection with data protection.

On March 31- April 1, 2005, the 37th Meeting of the International Working Group on Data Protection in Telecommunications took place in Madeira, Portugal. The most important matters dealt with at the Meeting:

- Latest development trends in the context of the national legislation of Member States;
- Provision of privacy rights in connection with the Internet services;
- Implementation of geographic localisation technologies on the Internet;
- Data protection and electronic voting;

- E-health and provision of privacy;
- Recent developments in connection with spam control and prevention etc;

Annual International Data Protection Commissioners Conference (Montreux, Switzerland)

The 27th International Conference of Data Protection and Privacy Commissioners took place on 14 -14 September in Montreux, Switzerland. It was organised by the Swiss Federal Data Protection Commissioner. Title of the Conference was: Towards the recognition of a universal right to data protection and privacy. Held for the first time in Switzerland, the Conference brought together more than 300 participants from across the entire globe. During the open sessions, representatives from the world of business, public administrations, science, the IT industry as well as governmental and non-governmental organisations engaged a debate with data protection and privacy commissioners from some 40 countries on the role of the right to data protection and privacy in a globalised world. During the closed session, the data protection and privacy commissioners adopted two resolutions whose purpose is to strengthen the compliance with personal data protection principles. One of the resolutions concerned the use of biometric data in passports, ID cards and travel documents. The other resolution concerned the use of personal data for political communication purposes.

More than at any time in the past, data protection has become the focus of debate and constitutes a major challenge of data protection authorities which has emerged as a result of the globalisation of our societies and the development of information technologies. Information exchange and access to data have become bywords for the functioning of companies and determine the success of many of the activities which we are called upon to perform. Modern technology allows information to be processed rapidly and in real time; at the same time it creates problems as to data protection.

It is important that at this international conference views and opinions may be shared not only among countries but also representatives of various sectors can take part, thus data protection issues are not left to the competence of data protection authorities only. The conference attendants held a joint opinion that discussions on data protection on the international level and passing this issue to the agenda of public and governments depends on the cooperation on the international level. Several attendants stressed that it becomes more and

more difficult to protect the right of the individual to privacy due to both the rapid development of technologies and the actions of the governments taken to ensure the state security. To ensure better protection of the right to privacy, the conference decided to focus on the following issues:

- Cooperation with the IT sector to implement common data protection standards;
- Problems faced by governments in connection with terrorism threats and data protection;
- Assessment of privacy in connection with the development of regulatory acts;
- Consumers and data protection policies;
- To stress the need of audits (inter alia technology audits);
- To use all the possibilities – like the World IT Summit in November 2005 – to facilitate the discussions on privacy protection and data protection.

It is planned that the Annual International Data Protection Commissioners Conference in 2006 will be held in Argentina.

Case Handling Workshops

In 1999, in Helsinki, the annual Spring Conference of European Data Protection Authorities took place; the conference adopted the decision to organise a seminar at which the case handling practice of European data protection authorities would be compared. The said principle of closer cooperation among European supervisory authorities of personal data protection arises from Article 28 (6) of Directive 95/46/EC, which stipulates the cooperation among the said authorities to perform their duties. In 2000, in Stockholm, Sweden, the 1st Complaint Handling Seminar, which is organised two times a year, took place; the seminar is attended by those officials of data

protection authorities who are dealing with complaints and draw up draft decisions on complaints. At the seminars, the attendants exchange information on complaint handling in every particular sphere. The seminar has an informative status and a report on the seminar is presented at the annual spring meetings of European data protection authorities.

From November 17 to 18, 2005, XII Case Handling Workshop took place in Paris, France; the workshop dealt with the current issues in the countries of the workshop members. Also representatives from the DSI attended the workshop. The main topics of the workshop were:

1. Recent developments in connection with the changes in the legislation on data protection;
2. Contribution of the delegations of Member States in connection with individual cases of cross-border complaints;
3. Reports of the European Data Protection Supervisor in relation to the latest developments within the European Union;
4. Contribution of the European Commission – complaints filed with the EC;
5. Data subjects and medical health files;
6. Latest developments and problems in connection with whistle-blowing schemes.

19th meeting of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, France)

Pursuant to the Law on the European Council Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 5 April 2001, Latvia has ratified European Council Convention No. 108 of 28 January 1981. In accordance with Article 18 of the Convention, a Consultative Committee (T-PD) shall be set up after the entry into force of the convention; Each Party appoints a representative to the committee. The Convention entered into force on October 1, 1985, and regular meetings of the Consultative Committee have taken place since that date. In-between the meetings, working

groups of the Committee have held meetings with the purpose to assess the priority issues raised by the T-PD.

Pursuant to the decision of 2003 on the necessity to consolidate the activities of the European Council with regard to data protection in order to ensure greater efficiency, the data protection committees were restructured upon agreement with the Working Group of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data to develop the T-PD as a joint data protection committee. Therefore, the T-PD meeting in 2004 was the first meeting the documents examined and approved by which were not to be dealt with by meetings of the European Council Data protection Projects Group, to which experts were invited from all European Council Member States, including those which had not signed or ratified the Convention. At the same time, within the European Council, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, T-PD-BUR, was established, and its task is to prepare draft documents for examination by annual meetings of the T-PD.

According with the agenda of the 21st meeting, the main task of the T-PD meeting in 2005 was to continue the discussion from 2004 on the opinion of scientists on the possibility to apply the principles of the Convention also in future in connection with the development of information technologies; also, the matter on data protection in connection with the development and application of biometry technologies was dealt with to prepare an opinion. As new countries are ratifying the Convention, the number of participants and observers of the meetings is growing; therefore, a more active work is expected within the meetings.

Visit of Parliament Members of the Czech Republic at the Data State Inspection

On November 1, 2005, the DSI was visited by Zuzka Rujbrova, Member of the Chamber of Deputies, Chairwoman of the Committee for Petitions of the

Parliament of the Czech Republic, and a number of representatives from the Commission.

Signe Plūmiņa, Director of the DSI, acquainted the guests with the work of the Inspection, the current experience of Latvia as to data protection and the cooperation with personal data protection supervisory authorities of the Central and Eastern Europe countries, in particular the Czech Republic.

During the meeting, issues related to the public opinion and awareness of their rights in relation to data protection, increase of the public informedness level, data transfer to countries where the personal data protection level is lower than in the EU, issues on the cooperation of among the supervisory authorities of personal data protection, and the use of identity numbers in public registers were discussed.

The Parliament Members expressed their interest about the role of the privacy institute in Latvia and the work carried out by the DSI in explaining the Personal Data Protection Law to the public.

10. Phare 2002 Twinning Project Data State Inspection

When the DSI commenced its work in 2001, there was a possibility to apply for an EU-financed cooperation project for raising the capacity of institutions. In the time period when Latvia prepared for the accession to the EU, institutions of the EU stressed the necessity to raise the capacity of officials of public administration authorities as one of the most substantial. Since the DSI was a newly-established government institution, it needed not only legal assistance for the development of various regulatory acts in connection with personal data protection but also practical recommendations on the work of the DSI. The implementation of Phare 2002 Twinning Project No.LV/2002/IB/OT-01 Data State Inspection (hereinafter – the Project) was commenced behind the time – only on September 15, 2004, when a number of the activities under the Project had been already carried out by the DSI in the four years (e.g. development of the audit manual, procedure for the circulation of internal information, public information strategies etc).

General objective of the Project – to strengthen the administrative capacity of the DSI in order to implement the *acquis communautaire* requirements with regard to personal data protection of the EU. One of the objectives under the Project was to develop the required amendments to the regulatory acts in order to ensure the compliance with the requirements under Article 28.1 of Directive 95/46/EC, which stipulates “Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them”.

The Project was implemented in cooperation with the Austrian Ludwig Boltzmann Institute of Human Rights. Signe Plūmiņa, Director of the DSI, was the Project Manager of the part of Latvia, and Hannes Tretter, Director of the

Ludwig Boltzmann Institute of Human Rights, was the Project Manager of the part of Austria, and Friedrich Lachmayer, Professor of the Innsbruck University, was the Practical Project Manager. For the implementation of the Project, the work of the resident twinning advisor, whose main task was to organise the project implementation procedure in cooperation with the DSI personnel and the short-term experts from Austria and Germany. Thomas Giesen, German data protection expert, former Head of the Sachsen Data Protection Authority, was elected the Resident Twinning Advisor.

In total 38 short-term experts from Austria and Germany took part in the implementation of the Project. The Project was implemented within the period from 15 September 2004 to 15 September 2005. The Project language was English, but the recommendations, manuals and strategies developed during the year were translated into Latvian so that specialists of various branches could read them.

The Project was implemented in four parts:

- 1) Improvement of the legal basis of the DSI;
- 2) Improvement of the operational basis of the DSI;
- 3) Strengthening of the capacity of the DSI;
- 4) Information and raising awareness on data protection issues.

The tasks fulfilled under the Project 'Data State Inspection':

- 1) the analysis on the existing legislation of Latvia in the sphere of data protection carried out by foreign experts, detection of shortcomings;
- 2) development of recommendations and proposals for the improvement of the personal data protection legislation in Latvia;
- 3) commentaries on the data protection legislation of Latvia;
- 4) preparation of the development strategy of the DSI (supplementing the existing development strategy);

- 5) preparation of manuals (internal information movement, system registration, complaint and submission handling);
- 6) experience exchange visits to German and Austrian data protection authorities;
- 7) preparation of the security audit of personal data processing systems manual (supplementing the manual prepared by the DSI);
- 8) development of the public information strategy of the DSI (supplementing the existing public information strategy);
- 9) preparation of informative materials for data controllers; seminars;
- 10) preparation of informative materials (for wider public);
- 11) seminars for judges.

Already in 2004, in cooperation with the Ministry of Justice and other state institutions, a number of activities were carried out: the analysis of the existing legislation in the sphere of personal data protection was commenced; the analysis of the functions and obligations of personal data protection supervisory bodies of 11 Member States was prepared; a discussion on the amendments to the Personal Data Protection Law required to expedite the registration procedure of personal data processing systems was commenced.

In 2005, the work on the assessment of regulatory acts was continued, the audit manual was improved and supplemented, and other informative materials included in the Project were prepared. Due to the delay in the implementation of the Project it was necessary to change the implementation schedule – the work was continued simultaneously in all four parts of the Project because a number of the short-term experts changed and in the result the implementation of a number of project activities was done in a shorter time and simultaneously, not successively, as it had been planned. Many project activities were carried out in summer 2005, which created another problem – many officials of public administration authorities of Latvia whom it was planned to engage in the Project were on vacation. It has to be admitted that the large number of short-

time experts engaged slowed down the implementation; for every expert had to be familiarised with the existing situation in Latvia, the experts had not been prepared prior to arrival and they could not learn about the work carried out previously by their colleagues. Due to the said the work overlapped.

During the implementation of the Project, the supervision over the activities carried out was provided. One of the supervisory mechanisms was the Supervisory Committee, which was composed of representatives from the Ministry of Justice, the Ministry of Finance, the Central Finance and Contracting Agency, two employees of the DSI, and the Project Practical Manager of the part of Austria. To ensure the implementation of the Project, cooperation was established with the Ministry of Justice and the Ministry of the Interior (in connection with personal data protection) and the Ministry of Economy.

Under the Project, not only information was exchanged among the employees of the DSI and data protection experts from the EU; also a student from Germany came to the DSI as a trainee and he could learn about the practical project implementation.

From the ex-post assessment of the Project, it can be concluded that the delayed implementation thereof was one of the main problems as well as the language barrier and the different styles of work (the spontaneous work of the Resident Twinning Trainee vs. the scheduled work of the DSI). Although the Project cannot be assessed as an obviously positive contribution to the strengthening of the capacity of the DSI staff and the implementation of the *acquis communautaire* of the EU, the experience obtained was an important factor for the growth of employees and the mobilisation of the existing resources. Interestingly, in the opinion poll among the personnel of the DSI on team work, several employees pointed out that a real team work had been achieved just when the Project was being implemented. The employees pointed out that it is necessary to improve the communication skills to improve the cooperation among co-workers and to realise the objectives of the Inspection more

efficiently. From the aspect of human resources, the implementation of the Project showed that the personnel of the DSI are able to mobilise their forces and coordinate their everyday work in a manner that allowed finding time for the implementation of the Project. From the practical aspect, the three experience exchange visits to Germany (Bonn, Kiel) and Austria (Vienna) were important for the personnel of the DSI. They provided an insight in the everyday work of data protection authorities of other EU Member States and new knowledge was gained. Awareness of their knowledge motivates the employees to achieve more and more; therefore, it can be considered as a positive aspect for the strengthening of the capacity of the DSI.

As several short-term experts of the Project pointed out, the personnel of the DSI have knowledge and experience, which is very useful in newly-established personal data protection authorities. At the same time, during their working visits to Latvia, foreign short-term experts pointed out that the experience obtained by the DSI would be used to solve some issues more efficiently at the institutions represented by them.

The cooperation of the DSI with foreign short-term experts as provided for in the Project took place only within a few project activities. Cooperation mainly took place in relation to documents prepared by the DSI, and the short-term experts then added their commentaries to them. Unfortunately, all the commentaries and opinions of short-term foreign experts on regulatory acts were based on the inaccurate interpretation of the legislation of Latvia provided by the Resident Twinning Advisor Assistant, not on the basis of the opinions of the DSI. Due to communication problems caused by imperfect translation (imprecise translations of regulatory acts of Latvia, selective translation during experience exchange visits and meetings with experts) imperfect commentaries and opinions were developed and the DSI obtained incorrect information. Therefore, when implementing any projects in future, the project language problem should be stressed.

Under the Project, attention was mostly paid to the studies and analysis of the regulatory acts of Latvia and the preparation of commentaries; comparatively little emphasis was placed on the necessity to raise the administrative capacity of the DSI. Due to the said, the training seminars for the personnel of the DSI on various data protection aspect as provided for in the Project were not organised. Throughout the project implementation, attention was focused only on the determination of the independent status of the DSI in the legislation; therefore, the main objective under the Project – to strengthen the administrative capacity of the DSI – was not fulfilled.

Benefits from the Project:

- the analysis on the existing legislation of Latvia in the sphere of data protection carried out by foreign experts;
- the prepared informative materials for public information on data protection issues;
- seminars on data protection for judges and for officials of law enforcement authorities.

Despite of all the difficulties experienced during the implementation of the Project, it was implemented and the DSI is planning also in future to attract financial and human resources of the EU in order to improve the work of the DSI; also, the DSI is planning to take part, within the scope of its competence, in other projects in the status of experts on personal data protection.

11. Information on the Use of Budget Funds

| No. | | Allocated under Law: | Actually theused |
|--------|---------------------------------------------------|----------------------------|---------------------|
| 1. | Income (total) | 587274 | 486747 |
| 1.1. | Subsidies from general income | 286704 | 286704 |
| 1.2. | Foreign financial help | 293070 | 199443 |
| 1.3. | Paid services and other income | 7500 | 600 |
| 2. | Expenses (total) | 587274 | 486746 |
| 2.1. | Remuneration | | 84418 |
| 2.1.1. | Salary | | 59793 |
| 2.1.2 | Bonuses | | 19710 |
| 2.1.3. | Benefits | | 4110 |
| 2.1.4. | Remuneration to non-staff employees | | 805 |
| 2.2. | Current expenses | | 258989 |
| 2.2.1. | Mandatory state social insurance contributions | | 17056 |
| 2.2.3. | Domestic business travels | | 0 |
| 2.2.4. | Foreign business travels | | 37934 |
| 2.2.5. | Services of national data transmission network | | 5535 |
| 2.2.6. | Other communication services | | 13966 |
| 2.2.7. | Health treatments costs paid by employer | | 4262 |
| 2.2.8. | Services related to security of administration | | 40126 |
| 2.2.9. | Repair of buildings, | | 1848 |

| | | | |
|---------|--------------------------------------------------------------------------|--|-------|
| | constructions and premises | | |
| 2.2.10 | Maintenance and repairs of means of transport | | 1431 |
| 2.2.11. | Technical maintenance and repairs of equipment, inventory and facilities | | 3515 |
| 2.2.12. | Maintenance of buildings and constructions | | 11780 |
| 2.2.13. | Mandatory third-party liability insurance of motor vehicles | | 374 |
| 2.2.14. | Payments for IT services | | 2089 |
| 2.2.15. | Lease and rent of premises | | 8787 |
| 2.2.16. | Other lease and rent | | 5586 |
| 2.2.17. | Other unspecified services | | 5608 |
| 2.2.18. | Payments for scientific research | | |
| 2.2.19. | Current expenses covered by foreign financial help | | 73359 |
| 2.2.20. | Other taxes and duties | | 45 |
| 2.2.21. | Office supplies | | 14800 |
| 2.2.22. | Inventory | | 365 |
| 2.2.23. | Heating | | 693 |
| 2.2.24. | Electricity | | 2115 |
| 2.2.25. | Petrol | | 4067 |
| 2.2.26. | Water supply and other energy materials | | 174 |
| 2.2.2. | Current repair and maintenance costs | | 3058 |
| 2.2.27. | Other materials | | 416 |

| | | | |
|--------|-----------------------------------------------------------|--|--------|
| 2.3. | Capital expenditure | | 143339 |
| 2.3.1 | Computers and calculators | | 5747 |
| 2.3.2. | Motor vehicles | | 0 |
| 2.3.3. | Office furniture and equipment | | 800 |
| 2.3.4. | Other movable property | | 673 |
| 2.3.5. | Intellectual property | | 10035 |
| 2.3.6. | Capital expenditures covered by foreign financial help | | 126084 |
| | Balance | | 1 |

|

12. Education and Training of Employees of the Data State Inspection

In the recent years great changes have been observed in different companies and organizations in both the private sector and the public sector. In nowadays, employees who can bear responsibility and provide the maximum results become more and more important instead of the hierarchy of organization. More and more often, when a new employee is recruited, first of all the professional conformity of the applicant is assessed and then his or her ability to work in team in order to achieve the goals set by the employer more efficiently.

In the recent years team work has also become more current in the state administration of Latvia – now it is one of the components of efficient state administration. Efficient state administration is an essential precondition for stable and well-balanced development of Latvia, to increase of international competitiveness and public welfare, and for active participation of the state within the European Union. In nowadays, the public demand the state administration to be easy accessible, reliable, its activities have to be transparent and comprehensible, and that it solved problems with respect to the uniqueness and specificity of each problem.

Employees of public administration institutions to a great extent are those who serve as a mirror for the society to which they serve for; therefore, the SDI has paid more attention to the possibilities of team work. The future aim of SDI is to become a prestigious institution in the eyes of both – its employees and the public. Continuous work with the staff is necessary to accomplish this task. Therefore, in 2005 the senior management of the SDI studied the factors that would motivate employees to continue working at the SDI and to put their efforts and forces to achieve the assessment of the public on the SDI as an expedient, professional and trustworthy institution. It has to be mentioned that the improvement of the work efficiency of organizations is longstanding question both in the private sector and the public sector; therefore, there have

been various attempts to implement activities set out clearly and in relevant procedures, as well as to improve the performance of each individual, however the search for the optimal solution is still continued.

A poll among the SDI personnel about a team work was carried out in 2005. A majority, or 90% of the inquired 15 employees of the SDI, considered that team is a group of individuals, who cooperate to achieve a shared goal; it is organized to accomplish through team-working those tasks that cannot be well-performed if each individual works separately. Therefore, not all tasks require a team work, thus it complies with the opinion of John Adair, who states that a real necessity to create a team emerges only when a task requires interaction of individuals, or otherwise the task can be simply accomplished by a skilled specialist. This statement proves to be true also in the everyday practice of SDI. A real team work was observed, for example, during the implementation of the Phare project mentioned above in this report, when employees had to learn to cooperate one with each other as well as with the foreign colleagues. Stimulation of the team work is only one of the possible solutions used to improve quality that is focused on at the SDI. Since the rotation of employees is increasing and there is the labour force emigration problem in Latvia, the SDI intends to make changes in the work of the Administration Department in 2006, paying more attention to the issue of human resources.

Within the reporting period, employees of SDI were provided with training opportunities. Most of the employees attended courses of lectures or took part in educational programs. The following training courses organised by the Latvian School of Public Administration and other educational establishments : Introduction Course for New Officials of State Administration; Personnel Management III – Auxiliary Interviews in Personnel Management: Complaint Interviews, Disciplinary Interviews, Consultation Interviews and Work Result Evaluation Interviews; Solutions of Written Conflicts and Stress Management; Emotional Intelligence and Management Skills; New Accounting Standards and Relation thereof to Annual Reports; Coming Remuneration Reform in the Public

Sector; Labour Law for Accountants; Computer Skills; Personnel Selection of and Integration into Team.

The personnel of the SDI are motivated to improve their knowledge. In 2005, 3 of 18 employees of the SDI had a higher education degree (lawyers), and 4 employees proceed with their studies to obtain an academic degree.

Distribution of employees by age:

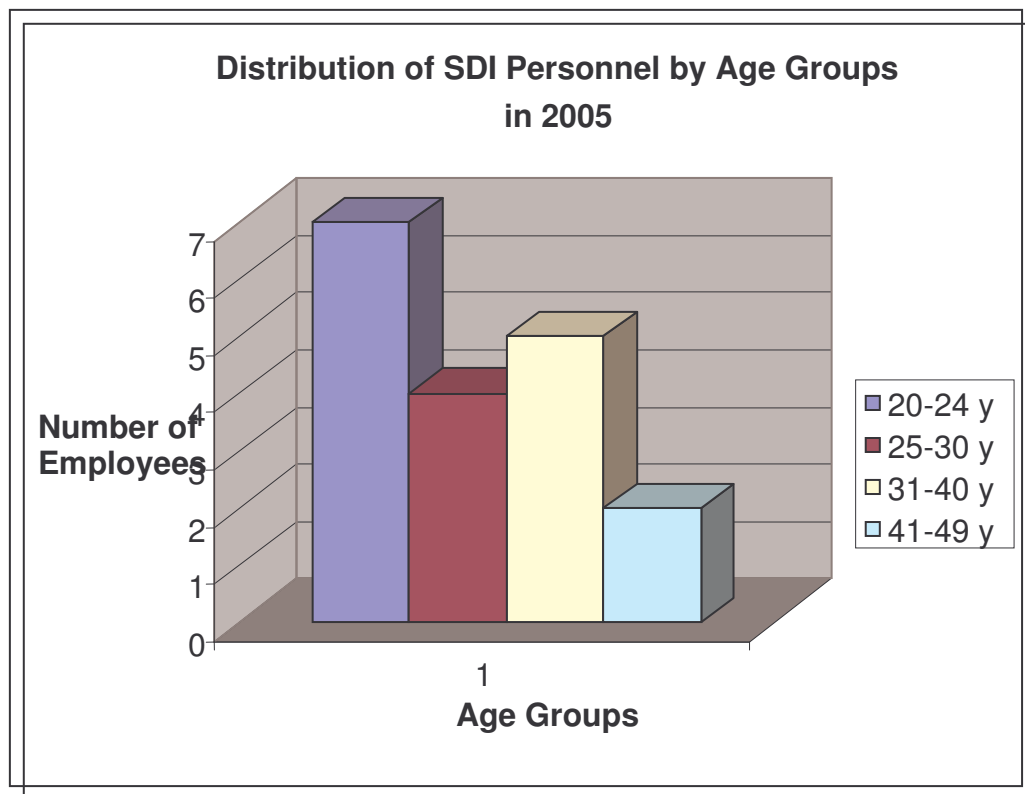
20 – 25 years – 7 employees

26 – 30 years - 4 employees

31 – 40 years – 5 employees

41 - 51 years – 2 employees

The average age of employees is 30 years.



Evaluation of Employees

SDI performs the evaluation of employees in compliance with the State Civil Service Law. The evaluation system of SDI employees was implemented in 2005. The evaluation of SDI personnel allows improving the efficiency of inspection's work and the employees work as good as possible and develop their

potential. The evaluation of employees gives an opportunity to the manager to distribute the professional responsibilities more appropriate among employees, to improve or to draw a career development design, thus decreasing the staff turnover, which is a very problematic issue in public administration authorities of Latvia. It is also planned to find out the opinion of clients about the work of SDI personnel in 2006. For the accomplishment of the evaluation an questionnaire, which included an evaluation and analysis on the fulfilment of duties, work results, and competences, was developed.

The evaluation of personnel is a responsible and psychologically peculiar process, therefore, the Administrative Department carried out explanatory measures in 2005 to avoid additional stress and negative attitude of employees at the work place. Employees were explained that all will benefit from the evaluation, because the main obstacles, problems and challenges in the labour process will be detected in the result, thus the evaluation can be considered also as an essential component for the improvement of the work quality. At the final stage of the evaluation, each employee had a chance to discuss the achieved results with the Director of the SDI in order to improve the efficiency of the work of the inspection in general.

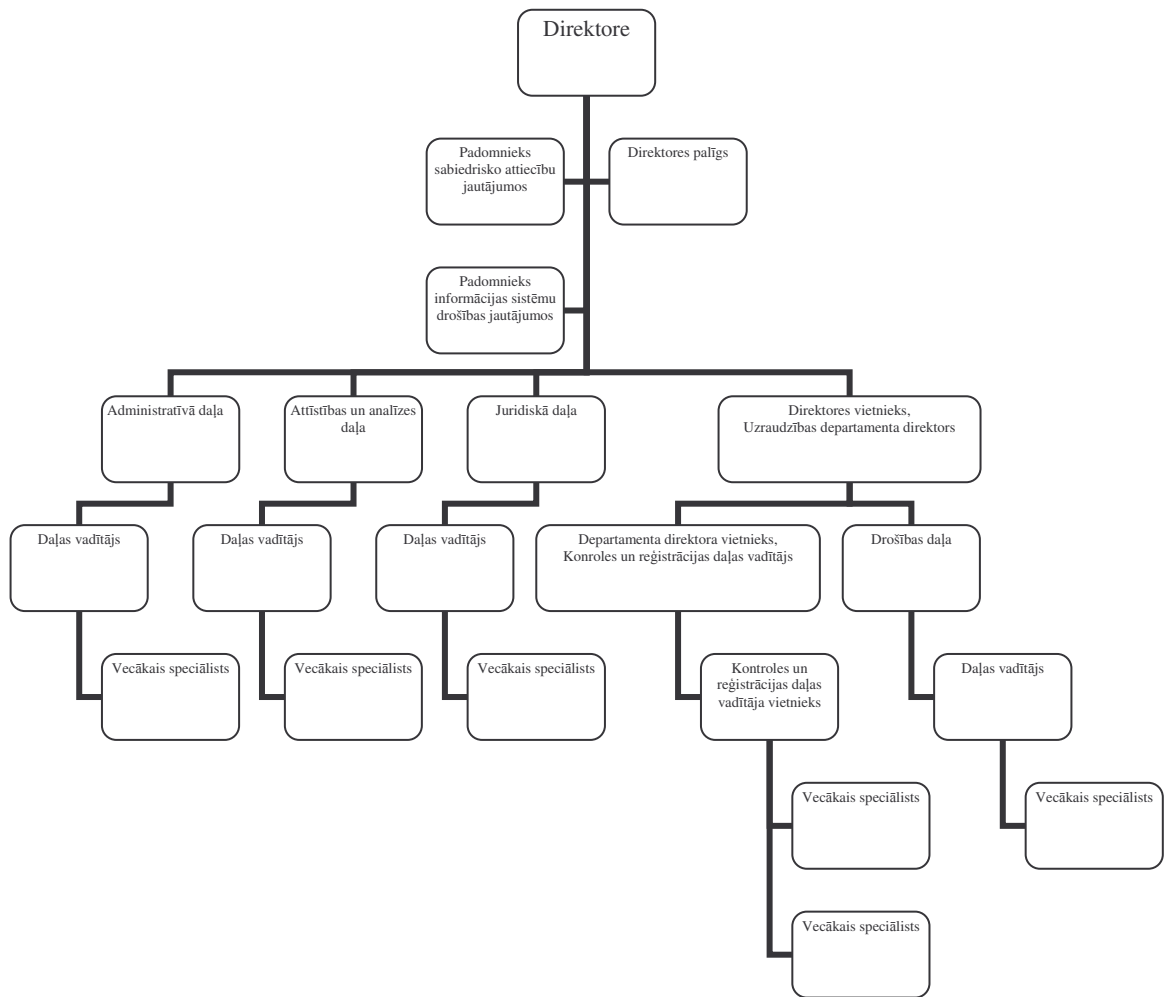
Reorganization of the Structure of the Data State Inspection

The reorganization of SDI structure was carried out in 2005 in order to optimise the internal management system of the SDI and to enable better coordination and performance of the mutual functions of the Registration Department, the Data Security Department and the Certification Service Providers Accreditation and Monitoring Department. The changes in the structure of SDI entered into force on May 2, 2005.

Structural Scheme of the DSI with Staff Units

Data State Inspection

| | | | | | | |
|------------------------------|----------------------------------------|-----------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------|------------------------|----------------------|
| | | | Director | | | |
| | | PR Advisor | Assistant Director | | | |
| | | Information Systems Security Advisor | | | | |
| Administrative Department | Research and Analysis Department | | Legal Department | Assistant Director, Director of the Supervision Department | | |
| Head | Head | | Head | Deputy Department Director, Head of the Control and Registration Department | Security Department | |
| | Senior Specialist | Senior Specialist | Senior Specialist | Deputy Head of the Control and Registration Department | Head | |
| | | | | | Senior Specialist | Senior Specialist |
| | | | | | Senior Specialist | |



13. Main Tasks and Planned Activities in 2006

1. To ensure that the privacy of guaranteed rights is respected and to ensure complete supervision of personal data protection in accordance with the requirements of the Law and the EU:

- To increase the number of registered systems;
- To increase the number of controls of personal data processing systems;
- To ensure that the infrastructure of the e-signature of the Ministry of Justice is developed;
- To ensure the accreditation of reliable certification service providers;
- To inform data processors on system audits. To facilitate the informedness of government and local government institutions on the obligation to carry out internal audits of personal data processing systems.
- To increase the number of audits of personal data processing systems of the government and local governments;
- To register the holder of the register of the domain .lv;
- To accredit auditors of personal data processing systems;
- To control the commission established by the main processor, which destroys the data, tissue samples, DNS descriptions and health condition records of gene donors and to take part in the committee's work (Cabinet Regulations No. 694, 10.08.2004);
- To ensure the supervision of the compliance with personal data protection requirements in the European Car and Driving Licence Information System (EUCARIS);

2. To facilitate the freedom of information;

- To initiate a cooperation project and implementation thereof in the sphere of freedom of information;

3. To improve the implementation of personal data protection regulations in government and local government institutions as well as in the private sector;

- To specify the provisions of the Personal Data Protection Law in relation to the implementation of legal norms of the EU by ensuring that the draft law is implemented and by developing a regulatory act on the transfer of data to third countries;
- To develop the legal regulation of the DSI in accordance with the amendments made to the Constitution in relation to the status of independent authorities;
- To ensure the accession of Latvia to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981 (ETS No. 108);

4. To facilitate the inclusion of personal data protection regulations in regulatory acts of sectors as well as the development of recommendations of individual sectors;

- To develop recommendations on data processing in the sphere of video surveillance, in the sphere of civil legal labour relationships, and the sphere of medicine and health treatment.

5. To improve the understanding of the public on the significance, tasks and objectives of personal data protection;

- To coordinate and supervise the implementation of the Freedom of Information Law and to ensure common implementation of the principle of the freedom of information in all government institutions;
- To inform the society on data security issues;

6. To ensure the strategic development of the legal system;

7. To provide comprehensive and clear information and recommendations on personal data protection:

- To issue the internal regulations of the DSI;

8. To improve and increase the efficiency of control, supervision policies and procedures;

- To carry out the measures required to make the information system of the DSI compliant with the security regulations of government information systems;
- To carry out the current risk analysis of the personal data processing system and to implement the required security measures;
- To register the register of personal data processing systems of the DSI with the Joint Register of State Information Systems;

9. To develop the procedures for the realisation of supervisory functions in compliance with the Electronic Communications Law;

10. To ensure the fulfilment of the national supervisory functions under the first pillar and the third pillar:

- To ensure the implementation of the Schengen Acquis Communautaire requirements in the legal regulation of Latvia and to ensure the course of the Schengen evaluation visit 'Data Protection' in 2006;
- To improve the personal data protection system to be ready for the supervision of the Schengen Information System and the Europol Information System;
- To control the implementation of the Customs Information System and conformity thereof to the requirements of the Personal Data Protection Law and the EU;

11. To improve and strengthen the participation in the Article 29 Working Party under Directive 95/46/EC;

12. To improve the cooperation with other international data protection authorities;

13. To supervise the transfer of personal data to third countries;

14. To find out the public opinion on personal data protection;

15. To support and facilitate the training and development of the personnel of the DSI:

- In accordance with the development of the DSI, to carry out the internal management control in accordance with the respective regulations and job descriptions;