FRA

Thematic legal study on assessment of data protection measures and relevant institutions Lithuania

Edita Ziobiene

Vilnius, Lithuania
February 2009

Contents

Executive summary

Overview

[1]. The right to protection of personal data is enshrined in Article 22 of the *Lietuvos Respublikos Konstitucija* [Constitution of Lithuania].[1] Among the most important guarantees of the inviolability of the private life of the individual are the provision in para. 3, 'Information concerning the private life of an individual may be collected only upon a justified court decision and in accordance with the law', and para. 4, 'The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life, and from encroachment upon their honour and dignity'. These provisions protect the private life of the individual against unlawful interference by the state, other institutions, their officers and other persons.

[2]. Lithuania is a member of several organisations which have an influence on the country's treatment of privacy and personal data. Lithuania has ratified and implemented a number of the relevant international instruments.

[3]. The basic legislative framework for data protection was established in the *Asmens duomenų teisinės apsaugos įstatymas* [Law on the Legal Protection of Personal Data],[2] which implements Directive 2002/58/EC.

[4]. Although data protection is regulated by the Constitution of the Republic of Lithuania, as well as national laws and international treaties, the mechanism for its practical implementation and the possibility of using and protecting this right in reality is of great importance. Deficiencies in practical implementation still exist.

Data protection authority

[5]. The Lithuanian data protection authority, the *Asmens duomenų apsaugos inspekcija* [State Data Protection Inspectorate], is a

[1] Lithuania/ *Lietuvos Respublikos Konstitucija* [Constitution of the Republic of Lithuania], approved by the Referendum of 25.10.1992, Parliamentary record, 1992-11-01, Nr. 11.

[2] The first version of *Asmens duomenų teisinės apsaugos įstatymas* [Law on the Legal Protection of Personal Data] was adopted on 11.06.1996 and the latest version of *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

government institution financed from the state budget. It is accountable to the government. The regulations of the Inspectorate are approved by the government.

[6]. The State Data Protection Inspectorate is headed by the Director. The Director of the Inspectorate is a civil servant, appointed through a competitive process for the period of office of five years, and can be dismissed by the Prime Minister in accordance with the procedure established in the *Valstybės tarnybos įstatymas* [Law on the Civil Service]. A person may be appointed to the post of the Director of the State Data Protection Inspectorate for no more than two periods of office. The Director must suspend his or her membership of any political party for the period of office.

[7]. The Law on the Legal Protection of Personal Data does not set out the requirements for a candidate for the directorship of the Inspectorate, the Law on the Civil Service sets out only the procedure for appointment. The fact that the law does not stipulate any requirements (education, experience or other) for the position of Director and the fact that the appointment decision is made solely by the Prime Minister should be noted as being very significant. This situation creates premises for political and other dependence. This report shows that this problem does indeed exist in reality.

[8]. The Inspectorate is responsible for the supervision and monitoring of the enforcement of the Law on the Legal Protection of Personal Data. The Inspectorate focuses mostly on the investigation of complaints. Other functions, such as data protection monitoring, research, advisory work and awareness-rising, are implemented unsystematically and inadequately.

[9]. The Law obliges data controllers and other legal and natural persons to immediately provide the information, documents and material necessary to carry out the Inspectorate's functions, if the Inspectorate requests this. The *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences] even provides sanctions for refusing to provide information[3].

[10]. Upon completion of an investigation, the Inspectorate makes a justified decision:

[3] Article 214(17) of *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences] provides that refusal of a request from the State Data Protection Inspectorate for information, documents and material necessary to carry out the Inspectorate's functions or obstruction of the Inspectorate in the exercise of its duties shall result in a fine of between LTL 100 and LTL 200 (about 29 to 58 Euro).

- to admit the complaint as justified;
- to reject the complaint;
- to dismiss the investigation of the complaint.

The decisions of the Inspectorate may be appealed against in a court in accordance with the procedure laid down in law.

Compliance

[11]. Data controllers and data processors must ensure the protection of personal data. Security of personal data comprises organisational, logical-technical procedures and measures to protect personal data and to prevent accidental or deliberate unauthorised destruction, modification or loss of data and unauthorised processing of such data. Data controllers must set out in their internal regulations the procedures and measures for security of personal data and shall define the individuals responsible for individual filing systems and the individuals who, by the nature of their work, will process individual personal data.

[12]. This study presents the legal requirements for processing special data, sensitive data (such as personal identification numbers) and processing personal data for very sensitive spheres (health care, social insurance, elections, evaluating solvency etc.), as well as registration for data processing.

[13]. The supervision of compliance for the duties regarding the registration of data processing operations and the duties of requesting approval for sensitive data processing operations are carried out by the State Data Protection Inspectorate and mainly through notification and permissions procedures, as well as orders and inspections.

Sanctions, compensation and legal consequences

[14]. Provisions on sanctions, compensation and legal consequences can be found in the Law on the Legal Protection of Personal Data[4] and the Code of Administrative Offences. [5]

[4] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[15]. The Inspectorate, upon the completion of an investigation, may hear cases of administrative offences and draw up a report of administrative offences. The court issues administrative sanctions on the basis of this report. This means that the Inspectorate investigates the violation and applies to the court. The court is responsible for the imposing of an appropriate sanction.

[16]. The Law on the Legal Protection of Personal Data[6] provides that any person who has sustained damage as a result of the unlawful processing of personal data or any other acts (omissions) by the data controller, the data processor or other persons violating the provisions of this Law shall be entitled to claim compensation for pecuniary and non-pecuniary damage caused to him/her. The extent of pecuniary and non-pecuniary damage shall be determined by a court.

Rights awareness

[17]. The field of personal data protection is relatively new in Lithuania, therefore there is an obvious lack of knowledge. Awareness-raising on all human rights issues is quite vague and Lithuania still needs to establish a national human rights institution for the protection and promotion of human rights, including protection of personal data.

[18]. The Inspectorate states that all information on its activity and on data protection may be found on its official website (www.ada.lt), but in reality the website contains very brief, superficial information, the monthly newsletters resemble press releases and the annual reports are rather short. On the official website it is written that the Inspectorate carries out training, but when the authors of this study asked for information about this over the last five years, the Inspectorate replied that it does not collect such information.

[19]. Awareness-raising is mostly organised by NGOs. However, this activity is not coordinated between the NGOs and is based only on projects financed by international donors. The state institutions do not organise or sponsor such activity. Because of this, human rights education and awareness-raising is chaotic and not systematic.

[5] *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences].
[6] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

Analysis of deficiencies

[20]. There are different types of deficiencies which are identified as a lack of human rights policy (including promotion and protection of personal data), the status and powers of the State Data Protection Inspectorate and the problematic interpretation of legal provisions.

[21]. Lithuania lacks a national human rights institution for the formation of human rights policy and the promotion and protection of human rights (including human rights monitoring, education, awareness-raising etc.) This situation creates additional problems, such as misunderstanding of the competences of the Ombudsman and other institutions and sometimes the overlapping of functions.

[22]. The status of the Inspectorate remains one of the biggest issues, since, as a governmental institution, it is more dependent on the government and has less respect in society compared with the Ombudsman institutions in Lithuania.

Good practice

[23]. NTR

Miscellaneous

NTR

1. Overview

1.1. Constitutional standards

[24]. The Preamble of the Constitution of the Republic of Lithuania (*Lietuvos Respublikos Konstitucija*)[7] proclaims that it strives for an open, just, harmonious civil society and state governed by the rule of law. The Constitution is to be considered an integral act (Article 6, para. 1 of the Constitution). The Constitutional Court has stated that the values and strivings enshrined in the Constitution are expressed in the constitutional norms and principles.[8]

[25]. The right to the protection of personal data and private life is established by Article 22 of the Constitution, which provides that :

'The private life of an individual shall be inviolable.
Personal correspondence, telephone conversations, telegraph messages and other intercommunications shall be inviolable.
Information concerning the private life of an individual may be collected only upon a justified court decision and in accordance with the law.
The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life, and from encroachment upon their honour and dignity.'

[26]. The Constitution establishes the inviolability of the private life of the individual, from which stems the individual's right to privacy. In its ruling of 21.10.1999 the Constitutional Court held that the individual's right to privacy encompasses private, family and home life, the physical and psychological inviolability of the individual, their honour and reputation, secrecy of personal facts and prohibition from publicising received or acquired confidential information etc. Among the most important guarantees of the inviolability of the private life of the individual are the provisions in para. 3 of Article 22 of the Constitution, 'Information concerning the private life of an individual may be collected only upon a justified court decision and in accordance with the law', and para. 4, 'The law and the court shall protect individuals from arbitrary or unlawful interference in their private or family life and from encroachment upon their honour and dignity'. These provisions protect the private life of the individual

[7] *Lietuvos Respublikos Konstitucija* [Constitution of the Republic of Lithuania], approved by the Referendum of 25.10.1992, Parliamentary record, 1992-11-01, Nr. 11.
[8] Ruling of the Constitutional Court of 11.07.2002, available in Lithuanian and English on the internet www.lrkt.lt *[January 10, 2009]*

against unlawful interference by the state, other institutions, their officers and other persons.

[27]. These constitutional provisions mean, *inter alia*, that the legislature has the duty to establish by law a procedure for the collection of information about the private life of individuals and the law must stipulate that information concerning the private life of an individual may be collected only upon a justified court decision.

[28]. Article 28 of the Constitution provides that, 'While exercising their rights and freedoms, individuals must observe the Constitution and the laws of the Republic of Lithuania, and must not impair the rights and freedoms of other people'. The Constitution permits the restriction of the constitutional rights and freedoms of the individual in the following circumstances: it is done by law; and the restrictions are necessary in a democratic society in order to protect the rights and freedoms of other persons and the values entrenched in the Constitution as well as the constitutionally important objectives. However, these restrictions do not deny the nature and essence of the rights and freedoms; the constitutional principle of proportionality is followed.

1.2. International standards

[29]. Lithuania is a member of several organisations which have an influence on the country's treatment of privacy and personal data. Lithuania has ratified and implemented a number of relevant international instruments.

[30]. The European Court of Human Rights has stated that interference in private life must be grounded in domestic law. However, domestic law must be in line with the principle of the supremacy of the law in a democratic state. The Constitutional Court noted that the jurisprudence of the European Court of Human Rights is an important source of the construction of law.[9]

[31]. As regards EC law, Lithuanian law complies with the requirements of Council Directive 95/46/EC.

[9] Ruling of the Constitutional Court 08.05.2000, available in Lithuanian and English on the internet www.lrkt.lt *[January 10, 2009]*

1.3. Legislation on data protection

[32]. Issues of personal data protection are regulated by the *Asmens duomenų teisinės apsaugos įstatymas* [Law on the Legal Protection of Personal Data],[10] which implements the Directive 2002/58/EC.

[33]. Other laws regulate personal data protection in specific spheres: the *Elektroninių ryšių įstatymas* [Law on Electronic Communication][11] provides protection of personal data in the field of electronic communication, the *Pacientų teisių ir žalos sveikatai atlyginimo įstatymas* [Law on the Rights of Patients and Compensation for Damage to their Health][12] etc. According to the Law on Electronic Communication,[13] the government should establish a resolution for the implementation of the law. Consequently, the government passed Resolution No. 807 of 20.07.2005, which approved the Rules for Inspections of Communication Secrecy, which specify the procedure for inspections carried out by the *Asmens duomenų apsaugos inspekcija* [State Data Protection Inspectorate] to establish whether the communication secrecy requirements of Article 63, para. 1, of the Law on Electronic Communication are complied with and also the procedure for formalising the results of such inspections.

[34]. It must be said that national debates on the effectiveness of the data protection system are initiated mostly by NGOs and certain institutions which have experienced monitoring by the State Data Protection Inspectorate. Discussions are vague. Parliamentarians hope that after the new amendments to the Law on the Legal Protection of Personal Data[14] many problems will be solved and that after six months new discussions on effectiveness of the data protection system may be initiated.

[10] The first version of *Asmens duomenų teisinės apsaugos įstatymas* [Law on the Legal Protection of Personal Data] was adopted on 11.06.1996, the latest version of *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[11] *Elektroninių ryšių įstatymas* [Law on Electronic Communication] 15.04.2004 No. IX-2135.

[12] *Pacientų teisių ir žalos sveikatai atlyginimo įstatymas* [Law on the Rights of Patients and Compensation for Damage to their Health], 03.10.1996 No. I-1562, latest amendment: 13.07.2004, No. IX-2361.

[13] *Elektroninių ryšių įstatymas* [Law on Electronic Communication] 15.04.2004 No. IX-2135.

[14] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

1.4. Institutional protection

[35]. The implementation of the Law on the Legal Protection of Personal Data[15] is supervised and monitored by the State Data Protection Inspectorate. The law sets out the status, mandate and powers of this institution (detailed information is provided in Section 2 'Data protection authority').

[15] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

2. Data protection authority

[36]. In accordance with the provisions of the Law on the Legal Protection of Personal Data,[16] the State Data Protection Inspectorate was set up in October 1996. Initially, the Inspectorate fell under the competence of the *Ryšių ir informatikos ministerija* [Ministry of Communications and Informatics], but in January 2001 the Inspectorate was reorganised into a separate authority of the government.

[37]. Article 36 of the Law on the Legal Protection of Personal Data[17] establishes that the State Data Protection Inspectorate is a government institution financed from the state budget. It is accountable to the government. The regulations of the State Data Protection Inspectorate are approved by the government. It means that the Inspectorate is established by the executive power and is not accountable to Parliament in its role of representing the nation. In other words, the Inspectorate is not accountable to society.

[38]. Article 37, para. 3, of the Law on the Legal Protection of Personal Data provides that state and municipal institutions and agencies, members of the Seimas (the Parliament), other officials, political parties, public organisations and other legal and natural persons shall have no right to exert any kind of political, economic, psychological or social pressure or other illegal influence on the Director of the State Data Protection Inspectorate or civil servants and employees employed under labour contracts. Interference with the activities of the State Data Protection Inspectorate shall entail liability in accordance with the law.

[39]. The State Data Protection Inspectorate is headed by the Director. The Director of the State Data Protection Inspectorate is a civil servant appointed through a competitive process for the period of office of five years, and can be dismissed by the Prime Minister in accordance with the procedure established in the *Valstybės tarnybos įstatymas* [Law on the Civil Service]. A person may be appointed to the post of the Director of the State Data Protection Inspectorate for no more than two periods of office. The Director must suspend his or her membership of any political party for the period of office.

[16] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[17] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[40]. The Law on the Legal Protection of Personal Data does not set out the requirements for a candidate for the directorship of the Inspectorate, the Law on the Civil Service sets out only the appointment procedure. The fact that the law does not stipulate any requirements (education, experience or others) for the position of Director and the fact that the appointment decision is made solely by the Prime Minister should be noted as being very significant. This situation creates premises for political and other dependence.

[41]. The post of Director is currently held by Algirdas Kunčinas, who was appointed in 2006 when the leader of the Social Democratic Party of Lithuania was Prime Minister. In the past Algirdas Kunčinas was twice[18] elected to the Parliament as a member of the Social Democratic Party of Lithuania.[19]

[42]. As mentioned above, the law does not provide any requirements for the position of Director. Algirdas Kunčinas is a philosopher and had not previously worked in the field of data protection or human rights issues[20]. Media and human rights NGOs are critical of this fact and believe that an incompetent Director cannot secure the quality of the Inspectorate's activity and may pass political decisions.

[43]. Some politicians blame the previous government (ruled by the Social Democratic party until the parliamentary elections in October 2008) and claim that the Annex to the Law on the Legal Protection of Personal Data was actually prepared specially for Algirdas Kunčinas. Article 2(4) of the Annex provides that, 'The Director of the State Data Protection Inspectorate taken into service before the entry into force of this Law shall, with his consent, hold the office after the entry into force of this Law. The period of office of the Director of the State Data Protection Inspectorate shall start to count from the date of entry into force of this Law'. Director Algirdas Kunčinas was appointed on 15.05.2006 and his term lasts till 2011, but the annex of the law prolonged his term till 2014. The authors of this report believe that this provision appeared to ensure that a member of the Social Democratic Party will keep this position even if the political climate should change after elections. This provision is very doubtful and shows that the Inspectorate is really a political institution.

[44]. The Inspectorate consists of five Divisions: the Complaints Investigation and International Cooperation Division, the Information

[18] 1992-1996 and 2000-2004.

[19] Algirdas Kunčinas' curriculum vitae is available on the website of the State Data Protection Inspectorate http://www.ada.lt/index.php?lng=en&action=page&id=58. *[January 10, 2009]*

[20] Algirdas Kunčinas' curriculum vitae is available on the website of the State Data Protection Inspectorate http://www.ada.lt/index.php?lng=en&action=page&id=58. *[January 10, 2009]*

and Technologies Division, the Law Division, the Prevention Division and the Finance, Accounting and Corporate Matters Division. The Inspectorate's staff has increased and since 2007 it has employed 34 members of staff (civil servants and regular employees).

[45]. Every year Parliament increases funding for the Inspectorate (see Annex 1) – in 2008 it was 2,060,000 Litas (596,617 Euro). Compared with the Ombudsman institutions, the Inspectorate's budget is much larger. The director of the Inspectorate decides how to use the budget.

[46]. It is very difficult to analyse whether the resources allocated to the data protection authority (budget, staffing etc) are sufficient to ensure effective use of the powers given to it. As mentioned above, the director has the right to appoint the necessary staff and decide how to use the budget. The problem is that the Inspectorate is not transparent and information about it is not made available to the public. In its annual report the Inspectorate identified two problems: low salaries of civil servants and the location of the Inspectorate.

[47]. The Inspectorate confirms that 17 per cent of its staff left their jobs in 2007. The reasons for this are as follows: the limited opportunities to pursue a career at the Inspectorate and the low salaries paid to civil servants (currently the Inspectorate has been classified as Group III, although it complies with the Group II criteria – it is ranked by the government). Moreover, the employees of the Inspectorate are highly qualified specialists, therefore they are in demand and welcomed by other state and private structures.[21]

[48]. The Inspectorate states that its location in two separate premises presents a negative factor for its activities. This impedes the proper maintenance of electronic communication infrastructure and hinders organising of meetings, workshops and client reception.

[49]. In its annual report the Inspectorate states that in 2007 it adhered to the strategic action plan for 2007-2009. All the targets set out in it were fulfilled, most of them exceeding 100 per cent. However, politicians, human rights NGOs and the media sometimes raise questions about the quality of the Inspectorate's activity and resent its decisions. On the other hand, data protection is a relatively new issue for Lithuanian society and needs deeper analysis, maybe this dissatisfaction is due to incomprehension.

[21] Lithuania/ *Asmens duomenų apsaugos inspekcija/ Annual report 2007*, http://www.ada.lt/index.php?lng=en&action=page&id=71. *[January 10, 2009]*

2.1. Powers and conformity with the Directive 95/46/EC

[50]. The powers of the State Data Protection Inspectorate are determined by the law. The Inspectorate is responsible for the supervision and monitoring of the enforcement of the Law on the Legal Protection of Personal Data (with the exception of Article 8) and also for the law on Electronic Communications section IX 'Personal data processing and privacy security' and the implementation of the provisions of the articles (with the exception of the provisions of Articles 63 (5), 65(4) and 70(7)). The Government of the Republic of Lithuania, by Resolution No. 1593 of 06.12.2004 entitled 'On granting authorisation for the implementation of the Law on Electronic Communications of the Republic of Lithuania', mandated through the Inspectorate (through Article 4) to undertake monitoring ensuring the inviolability of the private lives of the users of electronic communications, according to the procedures established by the government. The Government, by Resolution No.807 of 20.07.2005, approved the Rules for Inspections on Communication Secrecy, which specify the procedure for inspections carried out by the Inspectorate to establish whether the requirements to ensure communications secrecy set out in Article 63, para. 1, of the Law on Electronic Communication are complied with and also the procedure for formulating the results of such inspections.

[51]. Article 40 of *Asmens duomenų teisinės apsaugos įstatymas* [Law on the Legal Protection of Personal Data] provides the functions of the Inspectorate:

"

a administer the State Register of Personal Data Controllers, make its data public and supervise activities of data controllers relating to the processing of personal data;
b examine requests of persons in accordance with the procedure laid down in the Law on Public Administration;
c examine complaints and notifications of persons (hereinafter - complaints) in accordance with the procedure laid down in this Law;
d check the legality of personal data processing and make decisions concerning violations in personal data processing;
e grant authorisations to data controllers to transfer personal data to data recipients in third countries;
f draw up and announce annual reports on its activities;
g consult data controllers and draw up methodological recommendations on the protection of personal data and make them public on the internet;

h in accordance with the procedure laid down in the law, assist data subjects residing abroad;
i in the cases laid down in the law provide other countries with information about legal acts of the Republic of Lithuania on data protection and the practice of their administration;
j in the cases laid down in this Law, carry out a prior check and give conclusions to the data controller on the intended data processing;
k cooperate with foreign institutions in charge of protection of personal data, the European Union institutions, agencies and international organisations and take part in their activities;
l implement provisions of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);
m give proposals to the Seimas, the government, other state and municipal institutions and agencies for the drafting, amending and repealing of laws or other legal acts provided that their provisions concern issues falling within the competence of the State Data Protection Inspectorate;
n assess personal data processing rules presented by data controllers;
o discharge other functions established by this Law and other laws."

[52]. *Advisory function*. The Inspectorate may advise the Parliament, the government or other state institution on how to amend laws, how to solve problems related to data protection, raise problematic issues etc. But neither in the annual report nor in any other publicly available document is it possible to find any example of the Inspectorate giving advice to state institutions. Only on the Inspectorate's official website does it state that the Inspectorate actively negotiated with the government for the drafting of the new version of the Law on the Legal Protection of Personal Data, which was adopted on 01.02. 2008.

[53]. The Law on the Legal Protection of Personal Data does not establish a specific requirement for the Parliament and government to consult the Inspectorate when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, as required by Article 28, para. 2, of Directive 95/46/EC, but in practice the Parliament and government usually ask an opinion of competent national institutions and NGOs.

[54]. The Inspectorate issues an annual report and newsletters almost every month. The Law stipulates the right of the Inspectorate to consult data controllers and draw up methodological recommendations on the protection of personal data and make them public on the internet. In reality this function is implemented inadequately, there is very little information accessible to the public.

[55]. *Investigative powers and powers of intervention.* The Inspectorate focuses mostly on the investigation of complaints. (The detailed

statistics are provided in Annex 1.) Anyone who believes that his/ her rights were violated by the data controller has the right to lodge a complaint. The general requirement is that a complaint shall be lodged in writing, including electronic format (this means it must be signed with a secure electronic signature). If the Inspectorate receives an oral complaint or if it has established the existence of elements comprising a violation of the Law from the mass media or other sources, it may initiate an investigation on its own.

[56]. According to Article 43 (1) the complaint shall contain the following information:

"

1) addressee – the State Data Protection Inspectorate;
2) full name and address of the complainant and, if the complainant wishes, his/her telephone number or electronic mail address;
3) name of the complainant and address of its registered office or residence, or address of the place where data are processed;
4) description, time and circumstances of the act (omission) complained about;
5) the complainant's application to the State Data Protection Inspectorate;
6) date of the complaint and the complainant's signature.

The complaint may include the evidence available or a description of it.

[57]. Failure to keep to the format for a complaint referred to in Paragraph 1 of this article or to give the requisite information shall not form the basis for a refusal to investigate the complaint. Anonymous complaints shall not be investigated unless the Director of the Inspectorate decides otherwise.

[58]. The Inspectorate may take a decision to refuse to investigate the complaint within five working days of the date of receipt of the complaint and to notify the data subject, if:

" 1) the investigation of the circumstances referred to in a complaint falls outside the competence of the Inspectorate;
2) the complaint on the issue has already been investigated by the Inspectorate, except for cases when new circumstances are referred to or new facts are submitted;
3) a complaint on the issue has been investigated or is under investigation in court;
4) a procedural decision to start a pre-trial investigation of the subject of the complaint has already been made;
5) the text of the complaint is unreadable."

If the Inspectorate issues a decision to refuse to investigate the complaint, the reasons for the refusal must be specified in the decision and the complainant has the right to contest this decision.

[59]. A complaint must be investigated and a reply to the complainant given within two months of the date of receipt of the complaint, unless the investigation requires a longer period owing to the complexity of the circumstances indicated in the complaint, abundance of information or continuous character of actions complained about. In such cases, the period of investigation shall be extended but for not longer than two months. The entire period of investigation of a complaint may not be longer than four months. The complainant shall be informed of the decision of the Inspectorate to extend the period of investigation of the complaint. In any case, complaints must be investigated in the shortest possible period.

[60]. The Inspectorate is granted the right to request copies and transcripts of documents and copies of data and to be given access to all data, facilities related to the processing of personal data and documents necessary for the discharge of its function of supervision of personal data processing. The Law obliges data controllers and other legal and natural persons to deliver information immediately.

[61]. Article 214(17) of *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences][22] provides that refusal of the State Data Protection Inspectorate's request for information, documents and material necessary to carry out its functions, or obstruction of the Inspectorate in the exercise of its duties shall result in a fine of between LTL 100 and LTL 200 (about 29 to 58 euros).

[62]. Upon completion of an investigation, the Inspectorate makes a motivated decision:

- to admit the complaint as justified;
- to reject the complaint;
- to dismiss the investigation of the complaint.

[63]. The Decisions of the Inspectorate may be appealed against in a court in accordance with the procedure laid down in law. This principle corresponds to the requirements of Article 28, para. 3, of Directive 95/46/EC.

[64]. *Availability of decisions*. The decisions of the Inspectorate are not publicly available and only summarised information on investigations is published in the newsletters and on the website. The Inspectorate refuses (for reasons of confidentiality) to provide any information on its investigations or decisions, even in the case of justified request. The authors of this report also experienced such a refusal.

[22] *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences], amended 29.01.2004 No IX-1995.

[65]. *Power to engage in legal proceedings or to bring violations to the attention of the judicial authorities*. The Inspectorate has the right to apply to the courts or the prosecution office regarding violations of data protection. However, the Inspectorate did not provide any information about the exercising of this right in practice.

[66]. *Monitoring role.* Article 40 of the Law on the Legal Protection of Personal Data provides that the Inspectorate is granted the right to supervise the activities of data controllers relating to the processing of personal data and may initiate an investigation on its own.

[67]. *Awareness raising and reporting functions.* The field of personal data protection is relatively new in Lithuania, therefore there is obviously a lack of knowledge about this area. The Inspectorate aspires to improve the level of data protection and thus prepares recommendations for data controllers and data subjects, carries out training, provides consultations and issues press releases to the media regarding its activities. It informs the public on a regular basis about the authority's activities, identifies personal data processing irregularities, especially in state institutions and encourages people to take an interest in personal data protection and apply to the Inspectorate to defend their rights as data subjects. However, this function is exercised relatively rarely. It should be noted that it is relatively rare for data subjects to refer to the data controller in order to solve issues of data processing together, and data controllers, in the discharge of their functions and processing personal data, often underestimate the importance of the right to the inviolability of private life.

[68]. With the rapid expansion of information technologies, a problem that arises is how to facilitate their implementation and establish a secure legal environment in which the human right to privacy is defended as well as the individual's aspiration not to sustain damage as a result of careless processing of personal data. Electronic business initiatives, forms of electronic government, ongoing processes of modernisation in traditional businesses and the application of advanced technologies in the spheres of activity of the traditional economy drive a constant increase in public and private subjects deploying information technologies in their activities. More and more people tend to use services offered by the electronic environment. These services give rise to automatically processed personal data, resulting in threats to the individual's private life and consequently extending the scope of the Inspectorate's activities.

[69]. Article 28, para. 5, of Directive 95/46/EC stipulates that the national supervisory authority should draw up a report on its activities at regular intervals. The Inspectorate issues annual reports every year

and they are available on the website. However, it must be said that these reports are rather superficial.

[70]. *International cooperation.* In recent years the Inspectorate has intensified communication and cooperation with data protection institutions from the European Union and other countries.

[71]. The authors of this study think that if the allocated resources were to be used to ensure the effective execution of the Inspectorate's functions, it would be satisfactory. The Ombudsman for Equal Opportunities, the Ombudsman for Children Rights and the Ombudsman for Media receive smaller budgets. However, the problem is that almost half of the Inspectorate's employees are responsible for technological, financial or administrative tasks. The authors consider that the Inspectorate should make its activity more effective but with the same resources.

[72]. Formally the powers given to the Lithuanian supervisory authority meet the requirements of Article 28 of Directive 95/46/EC, but the Inspectorate should become more independent, use its powers more effectively, including its reporting function, and use its allocated resources more effectively.

[73]. The Law on the Legal Protection of Personal Data does not concern the establishment of the Working Party in relation to Article 29 of Directive 95/46/EC. The authors of this report did not find any government regulation and did not receive any response from the Inspectorate.[23]

[23] The authors of the report did not include this question in the initial questionnaire for the Inspectorate. When they later asked about it, the Inspectorate employee concerned explained that responding to a question takes time and did not answer.

3. Compliance

[74]. In principle, personal data may be processed only if provision is made for this by law or on the basis of the consent of the individual. Personal data may be processed if:

- the data subject has given his/ her consent;
- a contract to which the data subject is party is being concluded or performed;
- it is a legal obligation of the data controller under law to process personal data;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the exercise of official authority vested by law and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data are disclosed;
- processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless such interests are overridden by interests of the data subject.

[75]. According to Article 2 (1) of the Law on the Legal Protection of Personal Data[24] personal data means any information relating to a natural person, the data subject, who is identified or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

[76]. The data controllers and data processors must ensure the protection of personal data. Security of personal data comprises organisational and logical-technical procedures and measures to protect personal data and to prevent accidental or deliberate unauthorised destruction, modification or loss of data and unauthorised processing of such data. Data controllers must prescribe in their internal regulations the procedures and measures for the security of personal data and must define the persons responsible for individual filing systems and the persons who, due to the nature of their work, will process individual personal data.

[24] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

3.1. Registration of data processing

[77]. Article 34 of the Law on the Legal Protection of Personal Data[25] stipulates that data controllers shall be registered in the State Register of Personal Data Controllers. This State Register is administered by the State Data Protection Inspectorate.

[78]. The content of notifications of data processing by personal data controllers, the application procedure and the procedure for the registration of personal data controllers in the database of State register are regulated by *Vyriausybės nutarimas, kuriuo patvirtinti Asmens duomenų valdytojų valstybės registro nuostatai bei Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklės* [Regulations of the State Register of Personal Data Controllers and Rules for the Notification of Data Processing by Personal Data Controllers, approved by the Resolution of the Government of the Republic of Lithuania No. 262].[26]

[79]. Personal data may be processed by automatic means only provided that the data controller or his/ her representative, in accordance with the procedure established by the government, notifies the State Data Protection Inspectorate, except when personal data are processed:

"

1) for the purposes of internal administration;
2) for political, philosophical, religious or trade-union-related purposes by a foundation, association or any other non-profit organisation on condition that the personal data processed relate solely to the members of the organisation or to other persons who regularly participate in its activities in connection with the purposes of the organisation;
3) in cases when the processing of personal data is made by the media for the purpose of providing information to the public, artistic and literary expression is supervised by the Inspector of Journalist Ethics;
4) in accordance with the procedure laid down in *Valstybės ir tarnybos paslapčių įstatymas* [Law on State Secrets and Official Secrets][27]. "

[25] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[26] *Vyriausybės nutarimas, kuriuo patvirtinti Asmens duomenų valdytojų valstybės registro nuostatai bei Duomenų valdytojų pranešimo apie duomenų tvarkymą taisyklės* [Regulations of the State Register of Personal Data Controllers and Rules for the Notification of Data Processing by Personal Data Controllers, approved by the Resolution of the Government of the Republic of Lithuania] 20.02.2002, No. 262. Official gazette 2002, No.20-768; 2005, No. 144-5249.

[27] *Valstybės ir tarnybos paslapčių įstatymas* [Law on State Secrets and Official Secrets] 20.12.2007, VIII-1443.

This is pursuant to Article 1(3)(3) of this Law, with the exception of cases where such means are used only for transit of data through the territory of the Republic of Lithuania, the European Union or another state of the European Economic Area. In the case laid down in this subparagraph, the data controller must have a representative – an established branch office or a representative office – in the Republic of Lithuania which shall be bound by the provisions of this Law applicable to the data controller.)

[80]. Article 3 of the Law on the Legal Protection of Personal Data[28] establishes the requirements for personal data processing. The data controller must ensure that personal data are:

- collected for specified and legitimate purposes and are not later processed for purposes incompatible with the purposes determined before the personal data concerned are collected;
- processed accurately, fairly and lawfully;
- accurate and, where necessary, for purposes of personal data processing, kept up-to-date; inaccurate or incomplete data must be rectified, supplemented, erased or their further processing must be suspended;
- identical, adequate and not excessive in relation to the purposes for which they are collected and further processed;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed.

3.2. Processing of sensitive data

[81]. According to Article 2 (1) of the Law on the Legal Protection of Personal Data,[29] personal data means any information relating to a natural person, the data subject, who is identified or who can be identified directly or indirectly by reference to such data as a personal identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. The Law also provides a definition of so-called 'special categories of personal data'. *Special categories of personal data* means data concerning the racial or ethnic origin of a natural person, his/her political opinions or religious, philosophical or other beliefs, membership of trade union and his/her health, sexual life and criminal convictions.

[28] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[29] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[82]. One of the reasons for the amendment of the Law on the Legal Protection of Personal Data[30] was the practical problems with the implementation of the law, especially misinterpretation of the law by the Inspectorate. The Inspectorate tried to prevent the Central Electoral Commission from processing the personal data of candidates after the elections, but lost the case in the courts. The Inspectorate has issued ambiguous recommendations on various issues and, as a result, the legislator decided to establish more requirements for personal data processing in order to avoid disputes in future.

[83]. The Law on the Legal Protection of Personal Data[31] provides that special categories of personal data may be collected for statistical purposes only. Personal data collected for statistical purposes may be disclosed and used for purposes other than statistical ones in accordance with the procedure and in the cases laid down in *Statistikos įstatymas* [Law on Statistics][32].

[84]. *Use of the personal identification number*. The personal identification number is a unique sequence of digits. It is assigned to a person in accordance with the procedure laid down in *Gyventojų registro įstatymas* [Law on the Population Register][33]. According to Article 8 of this Law, the structure of the personal identification number when it is assigned shall be as follows: the first digit indicates the person's sex and the century of birth, the second and third denote the last two digits of the year of birth, the fourth and fifth denote the month of birth, the sixth and seventh denote the date of birth, the eighth, ninth and tenth the order number of entry into the Register of all persons born on the same date and the eleventh digit is the check-digit of the first ten digits. The personal identification number assigned to the individual is unique and remains unchanged. The personal identification number is entered in the individual's personal documents.

[85]. The Law on the Legal Protection of Personal Data[34] allows the personal identification number to be used when processing personal

[30] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[31] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[32] *Statistikos įstatymas* [Law on Statistics], 23.12.1999, No. VIII-1511.

[33] *Gyventojų registro įstatymas* [Law on the Population Register], revised version of the Law as of 16.03.1999 No. VIII-1085, entered into force 01.06.1999

[34] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

data with the consent of the data subject or without the consent of the data subject only if:

- such a right is laid down in this and other laws;
- scientific or statistical research is being undertaken;
- it is processed in state or institutional registers, provided that they have been officially set up in accordance with the procedure laid down in the Law on State Registers and in information systems provided that they have been set up in accordance with the procedure laid down in legal acts;
- it is processed by legal persons involved in activities related to the granting of loans and recovery of debts, insurance or financial leasing, health care and social insurance as well as in the activities of other institutions providing and administrating social care, educational establishments, science and educational institutions. Legal persons specified in this subparagraph may use the personal identification number only for the purpose for which it has been received and only in those cases where it is necessary for a legitimate and specified purpose of personal data processing;
- classified data are processed in cases laid down by law.

[86]. The personal identification number may not be made public, since it identifies the person's gender at birth (as mentioned above, the law does not allow changes, even if an individual changes gender) and date of birth. The personal identification number may not be collected and processed for direct marketing purposes.

[87]. *Personal data processing for health care purposes.* Personal data on an individual's health (state of health, diagnosis, prognosis, treatment, etc.) may be processed by an authorised health care professional. An individual's health shall be subject to professional secrecy under the *Civilinis kodeksas* [Civil Code], laws regulating patients' rights and other legal acts. Personal data processing for scientific medical research purposes shall be carried out in accordance with this and other laws. Personal data on a person's health may be processed by automatic means. Also for scientific medical research purposes the data may be processed only provided that the State Data Protection Inspectorate has been notified.

[88]. *Personal data processing for social insurance and social assistance purposes.* For the purposes of social insurance and social assistance, administrative institutions of the State Social Insurance Fund and legal persons providing or administering social assistance may exchange personal data without the data subject's consent.

[89]. *Personal data processing for the purposes of elections, referenda and citizens' legislative initiatives.* The processing of personal data (name, surname, date of birth, personal identification number, residential

address, citizenship, number of the identification document) for the purposes of elections, referenda, citizens' legislative initiatives, political campaigns and financing of political parties shall be regulated by this and other laws. Article 11 of the Law on the Legal Protection of Personal Data[35] provides that information compiled by the Central Electoral Commission on the basis of statements and other documents submitted by candidates or their representatives and announced on the internet about candidates, votes received by the candidates, lists of members of electoral or referendum committees, observers, representatives, members of initiative groups and lists of donors to political campaigns may be revised after the announcement of election or referendum results only for the purposes of correction of language mistakes or if the information on the internet differs from the information in the statements and other documents delivered at the time prescribed by legal acts. The personal identification numbers of the candidates and any other persons, their citizenship or numbers of their identification documents, the exact address (street, house and apartment number) of their place of residence may not be made public on the internet.

[90]. *Personal data processing for the purpose of evaluating a person's solvency and managing his/her debt*. Article 21 of the Law on the Legal Protection of Personal Data[36] provides that the data controller has the right to process and disclose to third parties with legitimate interests data, including the personal identification number, for data subjects who have failed to fulfil, in a timely and proper manner, their financial and/or property obligations (hereinafter 'debtors') for the purpose of evaluating their solvency and managing their debt, provided that data protection requirements set out in this Law and other legal acts are duly complied with. The data controller also has the right to disclose debtors' data, including their personal identification number, to other data controllers who process consolidated debtor files (hereinafter 'consolidated files'). The data controller may process consolidated files for the purpose of disclosing such data to third parties with legitimate interests so that they may evaluate the solvency of the data subject and manage his/her debt only if he/she, in accordance with the procedure laid down in Article 33 of this Law, has duly notified the State Data Protection Inspectorate which must carry out a prior checking weather such procedure is necessary.

[35] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[36] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[91]. The Law provides that the data controller may disclose debtors' data on condition that he/she has sent a written reminder to the data subject about his/her default and where, within 30 calendar days of the sending (submission) date of the reminder:

- the debt is not settled and/or the deadline for the repayment is not extended; or
- the data subject does not contest the debt on compelling grounds.

The data controller may not process special categories of personal data. Consolidated files may not be combined with personal data from other personal data files which have been compiled and are processed for purposes other than the evaluation of solvency and debt management.
The data about the default of the data subject in relation to a timely and proper fulfilment of his/her financial and/or property obligations may not be processed for a period longer than ten years from the date of settlement of the debt. Where the data subject repays his/her debt, data controllers must ensure that during the processing of data about the data subject's default in relation to the timely and proper fulfilment of his/her financial and/or property obligations the following information is specified:

- settlement of the debt by the data subject;
- the date of the debt settlement.

[92]. *Processing of data about financial services rendered in connection with risk acceptance for the purpose of solvency evaluation.* Banks and other credit institutions as well as financial undertakings engaged in credit and/or financial activities may disclose to each other the data subjects to whom these banks and other credit institutions, as well as financial undertakings who are engaged in credit and/or financial activities, have rendered or intend to render financial services concerning the acceptance of the risk (as laid down in the *Finansų įstaigų įstatymas* [Law on Financial Institutions][37]) (hereinafter 'services') Banks and other credit institutions as well as financial undertakings engaged in credit and/or financial activities may obtain personal data on the conditions and to the extent of paragraph 1 of this Article only if the data subject:

- applies to these institutions and undertakings for services or for the security of financial obligations;
- has received services from these institutions and undertakings or has given security for the financial obligations and it is necessary to evaluate the existence of risk for the proper fulfilment of the obligations undertaken.

[37] *Finansų įstaigų įstatymas* [Law on Financial Institutions], 10.09.2002, No. IX-1068.

Banks and other credit institutions as well as financial undertakings engaged in credit and/or financial activities shall ensure the data subjects' data received are not:

- processed for purposes incompatible with the purposes determined before the personal data concerned are collected;
- stored for a period longer than 12 months, if a negative decision concerning the granting of the service is taken.

Banks and other credit institutions as well as financial undertakings engaged in credit and/or financial activities shall ensure that data about the services rendered, performance and proper fulfilment of them are not stored for a period longer than ten years from the date of fulfilment of these obligations, unless laws or legal acts passed on their basis establish otherwise.

3.3. Supervision of compliance

[93]. The supervision of compliance with the duties regarding registration of data processing operations and the duties of requesting approval for sensitive data processing operations are carried out by the State Data Protection Inspectorate and mainly through notification and permissions procedures as well as orders and inspections.

[94]. The key objectives of the Inspectorate are supervision of data controllers' activities when processing personal data, monitoring the legality of personal data processing, prevention of violations in data processing and ensuring protection of the rights of the data subject.

[95]. Article 36, para. 4, of the Law on the Legal Protection of Personal Data[38] provides that the Inspectorate has no right to monitor processing of personal data in the courts.

[96]. The authors of this study cannot describe the requirements for the appointment of data protection officers, since the Law and the government resolution do not provide requirements for data protection officers and there is no other information publicly available. The authors believe that the Inspectorate conceals this kind of information in order to avoid doubts about its officers' abilities and knowledge. As mentioned above, data protection is a relatively new issue for Lithuania and in practice the Inspectorate has issued ambiguous decisions and recommendations and lost few cases in the courts. It may be for these reasons that the Inspectorate states that all

[38] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

information may be found on its website and refuses to provide any additional information.

[97]. It is hoped that all the problems in the supervision process will be solved with the coming into force of the amended Law on the Legal Protection of Personal Data[39].

[39] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

4. Sanctions, compensation and legal consequences

4.1. Legal bases

[98]. Provisions on sanctions, compensation and legal consequences can be found in the Law on the Legal Protection of Personal Data[40] and the Code of Administrative Offences. [41] The Law on the Legal Protection of Personal Data provides that violations of this Law shall render data controllers, data processors and other persons liable under the law.

[99]. Article 214(17) of the Code of Administrative Offences[42] provides that refusal of the State Data Protection Inspectorate's request for information, documents and material necessary to carry out the Inspectorate's functions, or obstruction of the Inspectorate in the exercise of its duties shall result in a fine of between LTL 100 and LTL 200 (about 29 to 58 Euro).

[100]. The Code of Administrative Offences[43] establishes for the State Data Protection Inspectorate the right to investigate cases of administrative offences if they are a violation of Article 214(14) of the Code of Administrative Offences.

[101]. Upon completion of its investigation, the Inspectorate may hear cases of administrative offences and draw up a report. On the basis of this report, the court issues administrative sanctions. This means that the Inspectorate investigates the violation and the courts are responsible for imposing an appropriate sanction.

[102]. Article 214(14) of the Code of Administrative Offences[44] provides that violation of the Law on the Legal Protection of Personal Data[45] in the

[40] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.
[41] *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences], amended 29.01.2004 No IX-1995.
[42] *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences], amended 29.01.2004 No IX-1995.
[43] *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences], Article 259(1).
[44] *Administracinių teisės pažeidimų kodeksas* [Code of Administrative Offences], amended 29.01.2004 No IX-1995.

processing of personal data shall result in a fine of between LTL 500 and LTL 1000 (about 145 to 290 Euro).

[103]. In general, the court applies an average fine if aggravating or mitigating circumstances do not exist.

[104]. Anyone who is suspected of an administrative offence retains a right to have an attorney. If the individual loses the case (that is, the court decides that he/she violated the law), he/she must pay the court fees.

[105]. It must be said that investigations depend largely on the personal initiative of data subjects. The law does not provide a consultation function for any state institution. This function is pro bono exercised by the Inspectorate and some NGOs, however no particular budget is allocated for this activity and NGOs do not have any possibility of applying for funding within Lithuania.

[106]. Since data protection is a relatively new issue, it is very difficult to confirm whether the courts and the Inspectorate analyse intention. Usually the court applies a general principle: in interpreting and applying laws, the court shall be guided by the principles of justice, reasonableness and good faith.

[107]. There is very little national case law as yet in the field of data protection. Court proceedings in this sphere are rare and no substantial information is available. The jurisdiction of the courts is mixed for these kinds of cases, since the first jurisdiction for cases of administrative offences (violation of the Law on the Legal Protection of Personal Data) lies within the courts of general jurisdiction, while appeals against these decisions lie within jurisdiction of the *Vyriausiasis administracinis teismas* [Supreme Administrative Court].

4.2. Compensation

[108]. The Law on the Legal Protection of Personal Data[46] provides that any individual who has sustained damage as a result of the unlawful processing of personal data or any other acts (omissions) by the data

[45] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

[46] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

controller, the data processor or other persons, which violate the provisions of this Law, shall be entitled to claim compensation for pecuniary and non-pecuniary damage caused to him/her. The extent of pecuniary and non-pecuniary damage shall be determined by a court.

[109]. The law does not provide the limits for compensation for pecuniary and non-pecuniary damage. In the past the Lithuanian Civil Code had a provision that the maximum compensation for non-pecuniary damage was 10,000 LTL (approx. 2,896 Euro), but compensation limits for non-pecuniary damage are now at the court's discretion.

4.3. Personal data protection in employment context

[110]. There are no particular legal provisions on the protection of personal data controlled and processed in the context of employment. The Law on the Legal Protection of Personal Data[47] provides the requirements for all data controllers and processors including employers.

[111]. When employers collect personal data about their employees they must comply with the principle of proportionality by processing only those data which are necessary and in their extent appropriate in relation to the purposes for which they are collected and processed.

[112]. Professional unions are more focused on solving other employment issues (salaries, taxes). The authors of this study did not find any information on participation by a professional union in a dispute about the processing of an employee's data.

[47] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

5. Rights awareness

[113]. The field of personal data protection is relatively new in Lithuania, therefore there is obviously a lack of knowledge. Awareness-raising on all human rights issues is rather vague, since Lithuania still needs to establish a national human rights institution for the protection and promotion of human rights.

[114]. The State Data Protection Inspectorate, aspiring to improve data protection level, prepares recommendations for data controllers and data subjects, carries out training, provides consultations and issues press releases to the media regarding its activities.

[115]. In order to develop its activities and to elicit public opinion about the quality of the service provided to its clients, the Inspectorate carried out a representative survey on the quality of the service provided by the Inspectorate in 2007. On its website, the Inspectorate states that the results of the survey illustrated that individuals as a rule refer to the Inspectorate for reasons of infringement of the rights of data subjects or the actions of data controllers or processors. Twice as many respondents hold the opinion that their concerns were treated fairly by Inspectorate employees as felt they were not treated fairly. (Percentage not provided.) The survey also revealed that all respondents were informed about actions taken by the Inspectorate in order to solve their complaints and 60 per cent of survey participants stated that this was done in a timely and proper manner. Thirty per cent of individuals surveyed considered that the Inspectorate works well or fairly well, while 20 per cent of individuals assessed the activities of the Inspectorate as very good. The majority of respondents expressed the opinion that information about the Inspectorate's activities is sufficient, although judging from responses it is obvious that the respondents would like to receive more thorough, detailed information concerning data protection. The respondents would like to find thorough information on data protection issues in the press, on the internet and on radio and television.[48]

[116]. The Inspectorate affirms that all information on the its activity and on data protection may be found on its official website (www.ada.lt), but it reality the website contains very brief, superficial information, the monthly newsletters look like press releases and the annual reports amount to only 17-20 pages. On the official website it is written that the Inspectorate carries out training, but when the authors of this study

[48] Lithuania/ *Asmens duomenų apsaugos inspekcija/ Annual report 2007*, http://www.ada.lt/index.php?lng=en&action=page&id=71 [*January 10, 2009]*

asked for detailed information about training over the past five years, the Inspectorate responded that it does not collect such information.

[117]. The documentation of the Inspectorate's investigations is not accessible to the public (the case files are confidential) and there is no library for those with an interest in the area (practising lawyers or students).

[118]. Awareness-raising campaigns are mostly organised by the NGO sector. For example, the Human Rights Monitoring Institute carried out a piece of long-term research (2004-2005) on the use of the personal identification number. Results from this research were published and disseminated for the public[49] and after this research the legislator changed the law. The Lithuanian Centre for Human Rights has organised a large number of seminars for different target groups on the right to private life and personal data protection. It also set up a special website (www.manoteises.lt) on human rights content, institutional protection and consultation.[50]

[119]. NGOs educate society about various human rights issues. But this activity is not coordinated among the NGOs and is based only on projects financed by international donors. The state institutions do not organise or fund such activity. Because of this, human rights education is chaotic and unsystematic.

[120]. Scientific institutions and universities do not carry out research on data protection issues.

[49] For further information see: http://www.hrmi.lt/en/project.php?strid=1044&id=2066.
[50] See www.lchr.lt and www.manoteises.lt.

6. Analysis of deficiencies

[121]. There are different types of deficiencies identified as a lack of human rights policy (including the promotion and protection of personal data), the status and powers of the State Data Protection Inspectorate and the problematic interpretation of legal provisions. It is hoped that some of these deficiencies will be reduced by the new legislation which came into force in the beginning of 2009. However, the status and powers of the Inspectorate still remain problematic.

6.1. Lack of human rights policy

[122]. Lithuania lacks a national human rights institution for the formation of human rights policy and the promotion and protection of human rights (including human rights monitoring, education, awareness-raising etc.). This situation creates additional problems, such as misunderstanding of the competences of the Ombudsman and other institutions and sometimes the overlapping of functions. For example, the Seimas Ombudsman (Parliamentary Ombudsman)[51] initiated an investigation into a complaint about the protection of the individual's right to good administration by the State Data Protection Inspectorate (the government agency) and received the reply from the Inspectorate, that the Seimas Ombudsman has no right to investigate the activities of the Inspectorate. On the other hand, the Inspectorate may start to investigate how the Ombudsman collects, processes and secures personal data. This example demonstrates lack of coordination and understanding between human rights protection institutions.

6.2. Problematic interpretation of legal provisions

[123]. As mentioned above, the Lithuanian Parliament adopted the amended Law on the Legal Protection of Personal Data on 01.02.2008, which came into force on 01.01.2009. This law complies with EU law. It is

[51] Article 12 of *Seimo kontrolierių įstatymas* [Law on the Seimas Ombudsman]. The Seimas Ombudsman investigates complaints concerning the abuse of office by, and bureaucracy of, officers or other violations of human rights and freedoms in the sphere of public administration and complaints about the actions of prosecutors and pre-trial investigation officers violating human rights and freedoms.

hoped that the new provisions will solve the practical problems which arose in the implementation of the previous version of this law.

[124]. Until 2009, the application of the Law on the Legal Protection of Personal Data was very complicated. Different interpretations and misinterpretation of existing laws had a negative influence on historical and other scientific research, the use of video surveillance, publishing of court decisions on official websites etc. The State Data Protection Inspectorate issued some controversial recommendations for state institutions, archives, the police and the courts on data protection issues. This led to the right to the protection of personal data becoming the most important value and it prevailed over state security or the dispensation of justice. The new version of the Law on the Legal Protection of Personal Data provides detailed provisions and it is hoped that the balance of constitutional values will be re-established.

6.3. Status and independence of the state data protection inspectorate

[125]. As was mentioned in Section 2 (Data protection authority), Article 36 of the Law on the Legal Protection of Personal Data[52] provides that the State Data Protection Inspectorate is a government institution, which is accountable to the government. This institution cannot be treated as an independent institution, since in reality it depends on the government and its political position.

[126]. As mentioned above, the Inspectorate as a governmental institution is more dependent on government and has less respect in society compared with the Ombudsman institutions in Lithuania.

[127]. The Director of the Inspectorate is a civil servant, appointed through a competitive process for the period of office of five years, and can be dismissed by the Prime Minister in accordance with the procedure established in the Law on the Civil Service. The Law on the Legal Protection of Personal Data does not set out the requirements for a candidate for the directorship of the Inspectorate, the Law on the Civil Service sets out only the procedure for appointment. The fact that the law does not provide any requirements (education, experience or other) for the position of Director and the fact that the appointment decision is made solely by the Prime Minister should be noted as

[52] *Asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatymas* [Law Amending the Law on the Legal Protection of Personal Data] was adopted on 01.02.2008 and came into force on 01.01.2009.

being very significant. This situation creates premises for political and other dependence. The post of Director is currently held by Algirdas Kunčinas, who was appointed in 2006 when the leader of the Social Democratic Party of Lithuania was Prime Minister. In the past Algirdas Kunčinas was twice[53] elected to the Parliament as a member of the Social Democratic Party of Lithuania. [54]

[53] 1992-1996 and 2000-2004.

[54] Algirdas Kunčinas' curriculum vitae is available on the website of the State Data Protection Inspectorate http://www.ada.lt/index.php?lng=en&action=page&id=58. *[January 10, 2009]*

7. Good practices

[128]. NTR.

8. Miscellaneous

[129]. NTR.

Annexes

Annex 1 – Tables and statistics

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority (in national currency, Litas)	389,000	660,000	724,000	864,000	1,074,000	1,652,000	1,781,000	2,060,000
Budget of data protection authority (in Euro)	112,662	191,182	209,685	250,232	311,052	478,452	515,813	596,617
Staff of data protection authority	8	22	22	24	30	30	34	34

Number of procedures (investigations, audits etc.) initiated by data protection authority on its own initiative	X[55]	86	165	233	365	63	92	97
Number of data protection registrations	X	X	X	X	X	X	X	X
Number of data protection approval procedures	X	X	X	X	X	X	X	X
Number of complaints received by data protection authority	X	X	23	X	91	119	161	154
Number of complaints upheld by data protection authority	5	8	21	55	87	102	121	129

[55] The 'X' symbol means that the State Data Protection Inspectorate did not provide any information. In its official letter (12.01.2009 No. 2R-45) the Inspectorate wrote that this information was not collected and is now impossible to provide. The same applies throughout this table where the 'X' symbol appears.

Follow-up activities of data protection authority, once problems were established (please disaggregate according to type of follow-up activity: settlement, warning issued, opinion issued, sanction issued etc.)	X	X	X	X	X	X	X	X
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)								

In its official letter (12.01.2009 No. 2R-45) the Inspectorate wrote that information on sanctions is not collected and is therefore impossible to provide.

Annex 2 – Case law

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

According to the State Data Protection Inspectorate Recommendations, state institutions cannot provide any decisions with personal data (including name and surname), because of it the courts and the Inspectorate provided decisions only with abbreviations of personal data. All final courts decisions are available without personal data. The authors of this study tried to obtain more complete information, but even a letter from FRA did not help.

Case title	The Police Department v. State Data Protection Inspectorate
Decision date	08.02.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	No. A[10]-140/2007, *Vyriausiasis administracinis teismas* [Supreme Administrative Court]
Key facts of the case (max. 500 chars)	In 1999 the Minister of Interior approved the Regulations for the use of the special database 'POLIS-CDB'. This database is used by police officers when they investigate criminal activities, administrative offences or fulfil other duties. The POLIS-CDB database contains the subsystem 'Relationship', which automatically provides all information from the Residents' register database and links to a family tree: providing personal information on the individual's grandparents, uncles, aunts, cousins and cousins' children. The Police Department states that this kind of information is very important when police officers investigate organised crime or use prevention means for organised crime. The POLIS-CDB database also contains information on everyone's administrative offences. The liability of administrative offences is valid for one year, but the database keeps information on everyone's administrative offences for a much longer, possibly unlimited, period of time.

Main reasoning/argumentation (max. 500 chars)	The Police Department as data controller must ensure that personal data are collected and processed for specified and legitimate purposes, which are necessary and not excessive in relation to the purposes for which they are collected and further processed. The subsystem 'Relationship' cannot be automatically used for the investigation of administrative offences, but it may be used in very special cases. However, the information on previous administrative liability may be kept in the database, since it is useful for characterising a person.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The decision explained that the Police Department as data controller does not have an absolute right to collect information, even to use it only for legitimate purposes.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court decided that the Police Department must ensure the security of personal data and use them only for legitimate purposes.
Proposal of key words for data base	Personal data, usage of database, legitimate purposes.

Case title	Armoniene v. Lithuania
Decision date	25.11.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	*Application no. 36919/02,* Judgement of the European Court of Human Rights

Key facts of the case (max. 500 chars)	The largest daily newspaper, *Lietuvos rytas*, published a front-page article entitled 'Pasvalys villages paralysed by the fear of death: residents of the remote Lithuanian area shackled by the AIDS threat'. In this article it was disclosed that the applicant's husband was 'already sick with this fatal disease' and giving his full name and address. The applicant claimed a violation of her husband's right to an effective domestic remedy, as the national law imposed a low ceiling on compensation for non-pecuniary damage caused by the unlawful public dissemination of information by the mass media about a person's private life – only 10,000 LTL (approx. 2,896 Euro)
Main reasoning/argumentation (max. 500 chars)	The Court noted that the publication of the article about the state of health of the applicant's husband, was of a purely private nature and therefore fell within the protection of Article 8. The Court attached particular significance to the fact that, according to the newspaper, the information about the husband's illness had been confirmed by employees of the AIDS Centre. The Court found that the severe legislative limitations on judicial discretion in redressing the damage suffered by the victim and sufficiently deterring the recurrence of such abuses, failed to provide the applicant with the protection that could have legitimately been expected under Article 8 of the Convention.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Court also acknowledged that certain financial standards based on the economic situation of the State must be taken into account when determining the measures required for the better implementation of the foregoing obligation. The Court likewise takes note of the fact that the Member States of the Council of Europe may regulate questions of compensation for non-pecuniary damage differently, as well as the fact that the imposition of financial limits is not in itself incompatible with a State's positive obligation under Article 8 of the Convention. However, such limits must not be such as to deprive the individual of his or her privacy and thereby empty the right of its effective content.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Found violations of Article 8 and awarded 6,500 Euro in respect of non-pecuniary damage plus any tax that may be chargeable, this sum being converted into the national currency of that State at the rate applicable on the date of settlement.
Proposal of key words for data base	Information on an individual's health, judicial discretion, redressing damage.

Case title	The State Data Protection Inspectorate v. G. B.
Decision date	14.04.2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	No. N^{3}-442-06, *Vyriausiasis administracinis teismas* [Supreme Administrative Court]
Key facts of the case (max. 500 chars)	The State Data Protection Inspectorate investigated a complaint. The complainant O. A. informed the Inspectorate that when she was changing 3,300 dollars into Litas in the NORD/LB bank she was asked to provide her passport and, without her consent, a copy of her passport was made. Because of this fact the Inspectorate applied to the courts. The bank states that it seeks to avoid being included on the list for money laundering and for this reason tries to identify every client if he/ she does not have an account at the bank and changes more than 2,500 Euro.
Main reasoning/argumentation (max. 500 chars)	The court noted that O. A., who wanted to change currency, and the bank acted as contractors and both parties of the contract understood that the currency may be changed only after the individual was identified. The Court also acknowledged that the Inspectorate did not provide any evidence that the bank processed O. A.'s personal data apart from for the contract (currency exchange). The Court also noted that the Inspectorate should write a report of administrative offences very carefully and justify what activity violated the law.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court decided to discontinue the case since an administrative offence was not identified.

Proposal of key words for data base	Data protection, report of administrative offence.

Case title	The State Data Protection Inspectorate v. J.J.
Decision date	30.06.2006
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	No. N 16 - 775 / 2006, *Vyriausiasis administracinis teismas* [Supreme Administrative Court]
Key facts of the case (max. 500 chars)	The complainant, R. K., informed the State Data Protection Inspectorate that when he/she was paying by card for goods (price exceeded 500 litas, 1,726 Euro) he/she was asked to provide his/her passport and, without his/her consent, the saleswoman wrote down the personal data: name, surname and personal identity number. Because of this fact the Inspectorate applied to the courts. The shop affirmed that its management had signed an agreement with the bank (SEB bankas), which states that when the price exceeds 500 litas, the salesperson shall prove the identity of an individual paying by card and copy from the passport individual's name, surname and personal identity number. The Inspectorate won this case in the first instance court (Vilnius City 2 district court). The court decided that the salesperson violated the Law on Data Protection and imposed an administrative sanction. However, the Supreme Administrative Court decided to dismiss the case, since the salesperson is not a data controller.

Main reasoning/argumentation (max. 500 chars)	The court noted that Article 214(14) of the Code of Administrative Offences establishes responsibility only for data controllers and the salesperson cannot be treated as data controller. The Court also noted that the Inspectorate should write reports of administrative offences very carefully.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The court analysed the difference between data controller and an individual who simply works according to their job specifications. The court also demonstrated that the Code of Administrative Offences lacks a provision regulating protection of personal data from disclosure by any individual.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court decided to discontinue the case since an administrative offence was not identified.
Proposal of key words for database	Data protection, report of administrative offence.

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).