

FRA

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

2 February 2009

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

# Contents

<b>FOREWORD .....</b>	<b>2</b>
<b>CONTENTS.....</b>	<b>2</b>
<b>EXECUTIVE SUMMARY.....</b>	<b>3</b>
<b>1. Overview.....</b>	<b>6</b>
<b>2. Data Protection Authority .....</b>	<b>8</b>
<b>3. Compliance.....</b>	<b>12</b>
<b>4. Sanctions, Compensation and Legal Consequences.....</b>	<b>13</b>
<b>5. Rights Awareness.....</b>	<b>15</b>
<b>6. Analysis of deficiencies .....</b>	<b>17</b>
<b>7. Good Practice.....</b>	<b>19</b>
<b>8. Conclusions .....</b>	<b>21</b>
<b>ANNEXES .....</b>	<b>23</b>

## Foreword

- [1]. The study was compiled by Ms Merle Haruoja, Ms Marianne Meiorg and Mr Kari Käsper, experts in Estonian human rights law. Ms Haruoja is Head of the Estonian Institute of Human Rights and Ms Meiorg and Mr Käsper work for the Human Rights Centre at the International University Audentes.
- [2]. The research team took into account all information available from publicly accessible sources. In addition, a formal Letter of Inquiry was sent to *Andmekaitse Inspeksioon* [the Estonian Data Protection Inspectorate, (EDPI)].
- [3]. The team used comparative and analytical approaches to the research subject. Relevant Estonian laws, regulations and practices were analysed.
- [4]. In general, it can be said that the EDPI was forthcoming in providing information. However, some information and statistics for the years 2000, 2001 and 2002 were unavailable.

## Executive summary

### Overview

- [5]. Protection of personal data is afforded sufficient protection in Estonian law. The right is expressly mentioned in the Estonian Constitution and Estonia is party to almost all Council of Europe data protection related international legal instruments.

### Data Protection Authority

- [6]. The primary law regulating personal data protection is the Personal Data Protection Act, which includes the data protection principles and specific rules regarding data protection. It implements Directive 95/46/EC completely as of its new version in 2008.

### Compliance

- [7]. The PDPA sets up the Estonian Data Protection Inspectorate (EDPI), which has an independent agency operating within the area of governance of the Ministry of Justice. The EDPI is managed by the Director General who is appointed by the Government on the basis of a recommendation of the Minister of Justice for the period of five years. There is a concern whether the appointment process is transparent and whether it is likely to undermine the independence of the EDPI. The EDPI has broad powers of investigation, either on its own initiative or as a consequence of a complaint. It is sufficiently staffed and structured to effectively carry out its obligations. The only concern is that the EDPI also monitors the fulfilment of the Public Information Act, and in case there is a necessity to dedicate more resources for that function, the data protection function might suffer a decreased availability of staff.

### Sanctions, Compensation and Legal Consequences

- [8]. There are both administrative and criminal sanctions for breaches of data protection rules. The sanctions are not used by the EDPI very

actively, as the approach seems to be to ensure that the data processor understands and complies with the rules. The statistics also show a minimal amount of fines issued. There is no specific compensation for data protection related civil damages; these are compensated according to regular compensation rules.

## Rights Awareness

- [9]. The EDPI has a recently updated website which includes not only information about the EDPI, but also large resources on international cooperation, all the precepts and decisions issued, advisory guidelines etc. The EDPI is involved with awareness-raising by organising conferences, however, the impact of this conference on society as a whole is limited.
- [10]. There is only one survey, conducted in 2006, which has specifically addressed the issue of the awareness of data protection. The survey showed that the awareness of the protection of personal data is low among the general population, and also rather low among the data processors themselves. People are aware of the right to turn to the EDPI, but they are not aware of the rights and principles of data protection.

## Analysis of deficiencies

- [11]. There is a possibility to appoint a data protection officer from 2008. However, it is unclear whether the persons appointed actually have the required expertise and training, and, more significantly, the independence required by the law.

## Good Practice

- [12]. The maximum fines for breaches of personal data processing rules were also raised tenfold from 2007 for legal persons. This allows for the data protection rules to have a bigger deterrent effect also for large companies.

# 1. Overview

- [13]. In Estonia, there are both constitutional and international standards with relevance to data protection. § 26 of the *Eesti Vabariigi Põhiseadus* [Constitution of the Republic of Estonia]<sup>1</sup> protects the inviolability of family and private life. It also states that “state agencies, local governments, and their officials shall not interfere with the private or family life of any person, except in the cases and pursuant to the procedure provided by law to protect health, morals, public order, or the rights and freedoms of others, to prevent a criminal offence, or to apprehend a criminal offender.”
- [14]. Estonia has been party to the European Convention on Human Rights and Fundamental Freedoms since 1998, to the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data since 2001 and to the 1997 Convention on Human Rights and Biomedicine since 2001. On 15 December 2008 Estonia signed, but has not yet ratified, the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows.
- [15]. The primary legislative act relating to data protection is the *Isikuandmete kaitse seadus* [Personal Data Protection Act] (PDPA),<sup>2</sup> the purpose of which, according to §1, is “the protection of the fundamental rights and freedoms of a natural person with regard to the processing of personal data, specifically the right for the inviolability of private life.” The PDPA provides for the conditions and procedure for the processing of personal data; the procedure for the exercise of state supervision over the processing of personal data and the liability for violation of the personal data processing requirements. The Agency tasked with implementation of the PDPA is the Estonian Data Protection Inspectorate (EDPI).
- [16]. A new version of the PDPA came into force on 01.01.2008. The Act completely replaces the old version which was in place up until the end of 2007. New features of the Act include a new division of personal data into ‘delicate personal data’ and ‘personal data’ (prior to 2008, the category of private personal data also existed), conforming with Directive 95/46/EC. The list of delicate personal data has been amended to include biometric data. Data subjects also have the right to demand a halt to publishing previously legally published data or using

---

<sup>1</sup> Estonia/*Riigikantselei* [State Chancellery] (28.06.2007) *Riigi Teataja* I, 43, 311.

<sup>2</sup> Estonia/*Riigikantselei* (16.03.2007) *Riigi Teataja* I, 24, 127.

data in any other way. In the field of publishing credit-related information, new rules allow publication of such information for up to three years commencing at the time of a person's credit problem. Maximum fines for data protection related breaches were increased tenfold, and it is now possible to fine legal persons up to 500,000 *kroons* (ca. 32,000 EUR) for data protection related breaches.

- [17]. The first personal data case involving a breach of processing personal data ended in June 2008. The case involved the publication of personal data of a former debtor to the commercial bank, AS Hansapank, on the credit information website *Krediidiinfo.ee*. The Data Protection Inspectorate, acting upon a complaint by a former debtor, issued an injunction to stop the publication of the data after the debtor had paid the debt, arguing that the bank had not properly asked for permission. The bank contested the injunction in court, but in June 2008 the Tallinn Circuit Court decided in favour of the Inspectorate, as did the Tallinn Administrative Court in April 2007. The decision has now become final.<sup>3</sup>
- [18]. The national debate regarding data protection became more active after controversial public statements were made by the EDPI in 2008 regarding the banning of birthday congratulations and death announcements on radio and the prohibition of publication of lists of people admitted to universities. This drew significant public criticism, which was partly caused by unclear statements by the EDPI, but also larger ignorance or negative opinion towards data protection rules (or human rights in general).

---

<sup>3</sup> Estonia/*Andmekaitse Inspeksioon* (17.07.2008) *Pressiteade* [press release] 3/2008, available at <http://www.dp.gov.ee/document.php?id=783> (25.07.2008).

## 2. Data Protection Authority

- [19]. The Estonian Data Protection Inspectorate (EDPI) is a government agency operating within the area of government of the Ministry of Justice that exercises state supervision of the processing of personal data, management of databases and access to public information and the discharge of other functions imposed by law or on the basis of law. The expenses of the Inspectorate are covered by the state budget. The budget of the Inspectorate is approved and amended by the Minister of Justice, who also assesses its execution. The EDPI is managed by the Director General, who is appointed to office by the Government of the Republic on the basis of the recommendation of the Minister of Justice for five years. The EDPI consists of three departments: development and analysis department, control department and general department. The EDPI has a total of 31 members on staff.<sup>4</sup>
- [20]. The powers of the EDPI correspond to the requirements of Article 28 of the Directive 95/46/EC. According to § 9 of the Statute of the EDPI, the primary functions of the EDPI include participation in the development of legislation related to its area of activity, the proposal of amendments and supplementations to such legislation as well as participation in the development of policies, strategies and development plans related to its area of activity; preparation and implementation of projects related to its area of activity, including participation in preparation and implementation of international projects. These functions correspond to those set out in Article 28(2) of Directive 95/46/EC.
- [21]. According to § 33(3) of the PDPA, the EDPI exercises state supervision over the observation of requirements deriving from the legislation regulating data protection and, if necessary, application of enforcement of powers of the state, which includes the powers mentioned in Article 28 (3) of Directive 95/46/EC. More specifically the EDPI can demand, according to § 33 (2) of the PDPA, the relevant documents and other necessary information from persons and make copies of the documents, apply, if necessary, the organisational, physical and IT security measures to protect personal data, as well as suspend or prohibit processing, demand rectification of inaccurate data, and demand the blocking or the termination of processing of personal data (including destruction or transfer to archives). A competent official of the EDPI has the right of unhindered access to inspect the territory or rooms of processors, the right to obtain access

---

<sup>4</sup> §1 of the *Andmekaitse Inspektiooni põhimäärus, struktuur ja koosseis* [Statute, Structure and Composition of the Estonian Data Protection Inspectorate] - Estonia/*Riigikantselei* (19.05.2008) *Riigi Teataja* I, 17, 266.



to the documents and equipment of processors, including recorded data, and to software used for data processing (§ 33 (3)). The EDPI has the right to issue precepts and make administrative decisions. According to § 40 of the PDPA, these can be appealed to the court by the subject of the precept or decision.

- [22]. The EDPI also can receive complaints from individuals, which must normally be resolved within 30 days. This complies with Article 28(4) of Directive 95/46/EC.
- [23]. Within the field of data protection, EDPI has a broad remit, fully in compliance with Directive 95/46/EC. There are no limitations which would significantly impede its remit.
- [24]. The budget and staff of the EDPI are sufficient at the moment and there have been no serious issues with the financial or administrative capacity within the last year. This is partly due to the relative novelty of data protection regulation. In the future, further resources might be needed to cope with an increasing number of cases and complaints. The EDPI also is the supervising authority for the *Avaliku teabe seadus* [Public Information Act] that guarantees access to public information.<sup>5</sup> There may be concerns regarding the allocation of resources, staff and budgeting within the EDPI between these two areas in such a way that the data protection function may suffer.
- [25]. § 33 of the PDPA states that the EDPI is independent in exercising its obligations and acts on the basis of the constitution, the law and legislation enacted pursuant to the former. § 16 (1) of the Statutes of EDPI confirms that the Director General of the EDPI is independent in exercising his or her obligations and acts on the basis of the constitution, the law and legislation enacted pursuant to the former. However, the budget of the EDPI is administered through the Ministry of Justice, which may be a tool for indirect influence of the EDPI by the government. There is also a concern regarding the selection process of the Director General of the EDPI. The appointment of the new Head of the Estonian Data Protection Agency in 2008 has also been controversial as the public competition required candidates among other things to be “oriented to the interests of the state”, which might be interpreted as contradictory to the requirements of independence and impartiality.<sup>6</sup>

---

<sup>5</sup> Estonia/*Riigikantselei* (08.12.2000) *Riigi Teataja* I, 92, 597.

<sup>6</sup> *Riigikantselei* (29.01.2008) *Avalik konkurss: Andmekaitse Inspektsiooni peadirektor* [Public competition: Head of the Estonian Data Protection Agency], available at: <http://www.riigikantselei.ee/tan?id=73200> (23.01.2009).

- [26]. The EDPI also publishes a yearly annual report of its activities. It is required to submit the annual report to the *Riigikogu põhiseaduskomisjon* [Constitutional Committee of the Parliament] and to the õiguskantsler [Chancellor of Justice]. The report is also published on the website of the EDPI.
- [27]. According to § 33 (5) of the PDPA, the EDPI can initiate proceedings based on a complaint or upon its own initiative. It can carry out inspections to monitor compliance with personal data processing requirements according to § 39 of the PDPA. Since 2008, the EDPI has started to become more proactive, however, about 90% of proceedings are still initiated as a reaction to complaints (see also Annex 1 statistics).
- [28]. The EDPI monitors data processors by means of random inspections, in many cases violations are detected due to a complaint or media enquiries. The EDPI has stated that 75% of inspections in 2007 were made upon its own initiative.
- [29]. All of the precepts and decisions on challenge made by EDPI are available on the website of the EDPI starting from January 2006. The website also includes advisory guidelines. There are no problems with access to information within the EDPI, especially as they are also tasked with supervision of access to public information.
- [30]. The Article 29 Working Party represents a source of inspiration for the EDPI. The Opinions of the Article 29 Working Party are provided for reference on the website of the EDPI and have been used and referred to within the opinions and guidelines of the EDPI.<sup>7</sup>
- [31]. The EDPI has a statutory mandate to be involved with legislative drafting in the field (§ 9 of the Statutes of the EDPI). It participates in the development of legislation, and proposes the amendments and supplements to such legislation; it also participates in the development of policies, strategies and development plans. It seems that the EDPI contributes effectively in the field and that in general, there have been no publicised concerns that the EDPI has been refused to be included in any legislative drafting related to data protection. In practice, no specific examples of the advisory role can be identified.
- [32]. One of the main awareness-raising activities is the EDPI yearly conference on the data protection day (28 January), which focuses on a topical issue of data protection.<sup>8</sup> The conference in 2007 was titled

---

<sup>7</sup> See: <http://www.aki.ee/est/?part=html&id=69> (23.01.2008).

<sup>8</sup> More information on the conferences see: <http://www.aki.ee/est/?part=html&id=25> (23.01.2009).

*“Isikuandmete kaitse ja e-riik”* [“Data Protection and e-State”] and in 2008 *“Isikuandmete kaitse ja meedia”* [“Data Protection and the Media”] and in 2009 *“Veebikäitumise piiramatul vabadus vs riskid”* [“Unlimited Freedom of Internet Activity vs Risks”].

- [33]. The EDPI further raises awareness through articles in the media as well as through its website and published guidelines. There have been no large-scale data protection campaigns, except for an internet based campaign which educates children, parents and teachers on the threats for young people on the Internet<sup>9</sup> as well as an outdoor media campaign on the issue of identity theft.

---

<sup>9</sup> See: <http://www.peremeedia.ee/> (29.01.2009).

### 3. Compliance

- [34]. For the processing of sensitive data, the processor must register with the EDPI, unless a person responsible for data protection has been appointed (§ 27 (1) of the PDPA). The processing of sensitive personal data is registered within 20 days, for a period of five years. According to § 29 of the PDPA, the EDPI may inspect the readiness of the processor for processing sensitive personal data prior to registering. In this case the registration may take an additional 10 days. There is no evidence available regarding compliance in practice.
- [35]. The abovementioned registration requirement is not necessary if a person responsible for the protection of personal data has been appointed according to § 30 of the PDPA. Any such appointment must be communicated to the EDPI without delay, including his or her name and contact information. This person must be independent from the processor in his or her activities and must ensure the data processor's compliance with the PDPA. There are no other requirements for the persons responsible for data protection, nor are there specific training programmes. There is no evidence as to whether these data protection officers have in practice the expertise required to fulfil their roles effectively.
- [36]. In practice, there is no information regarding how many processors actually fulfil the requirement of registration. There have been less than 100 data processors, where a responsible person has been appointed.
- [37]. For personal data, which is not sensitive, there is no mandatory registration of data processing.

## 4. Sanctions, Compensation and Legal Consequences

- [38]. The sanctions include both administrative sanctions within the PDPA and criminal sanctions within the *Karistusseadustik* [Penal Code].<sup>10</sup> The sanctions available under Article 42 of the PDPA include fines for the violation of the obligation to register the processing of sensitive personal data, failure to fulfil requirements for sending data abroad, breach of the obligation to inform the data subject, violation of the requirements regarding security measures to protect personal data, or other violations are punishable with a fine of up to 18 000 Estonian kroons (1 150 EUR) for individuals and of up to 500 000 Estonian kroons (31 956 EUR) for legal persons. There are no specific provisions to take account of negligence or intent.
- [39]. There is also a possibility for criminal sanctions for data protection related breaches. § 157<sup>1</sup> of the Penal Code includes, since 2007, a punishable crime for the illegal publication of, the allowing of access to or the transmission of sensitive personal data, where this has been done for personal gain or has resulted in substantial damages for another person's interests or rights. The maximum punishment is imprisonment for one year or monetary penalty. There are no cases that the rapporteurs are aware of in which any persons have been prosecuted for this offence. It is also doubtful whether there is enough awareness and expertise in data protection issues among the police for the successful application of the provision. The provision can also be interpreted widely, therefore the threshold for potential breaches of it is unknown.
- [40]. No specific provisions for compensation payments are included within Estonian law for data protection related breaches. None have been issued by the courts in data protection cases as there have been very few of these in total.
- [41]. The general procedure when a violation which does not give rise to criminal liability has been detected, is to issue a precept, which allows time to remedy the violations. Where the precept has not been complied with, fines can be considered. However, regarding the low amount of money received by the EDPI for fines, it seems that the EDPI is reluctant to use the fine as a sanction, except as a final resort.

---

<sup>10</sup> Estonia/Riigikantselei (2001) *Riigi Teataja* I, 61, 364.

- [42]. Enforcement depends largely on the personal initiative of data subjects to file complaints at the EDPI. It is the EDPI who then decides whether or not to act and it is the EDPI against whom the legal proceedings will be initiated by the data processor if they are unsatisfied with the precept of fine. There is no cost for the complainant, but he or she is also not in control of the proceedings, so the risk is completely on the EDPI. There are no specialised data protection NGOs which provide assistance in data protection cases.
- [43]. There are currently no special provisions in Estonian law regarding data protection in the context of employment. However, in the new *Töölepingu seadus* [Employment Contract Act],<sup>11</sup> which will be in force from 1 July 2009, § 41 imposes an obligation on the employer to ensure that the personal data of the employee is processed in accordance with the PDPA. The unions have no role in monitoring compliance with the PDPA either in law or in practice.

---

<sup>11</sup> Estonia/*Riigikantselei* (21.01.2009) *Riigi Teataja* I, 5, 35.

## 5. Rights Awareness

- [44]. There was a survey conducted in December 2006 regarding the awareness of the general population and of organisations of the protection of personal data.<sup>12</sup> The survey was conducted by *Turu-uuringute AS* and it involved interviews with 999 individuals and 154 representatives of a company or organisation. The target group was members of the public aged 15-74 and companies and organisations involved in the processing of personal data.
- [45]. The conclusions of the survey showed a lack of awareness regarding all aspects of data processing within the majority of the population. This includes when data can be collected, what is processing, what is sensitive personal data, etc. However, almost a half of the population was aware of the possibility to lodge a complaint at the EDPI. The results in relation to data processors showed that the processors were in general aware of the laws and regulations as well as the need for protection of personal data. However, many processors lacked a clear understanding of the specifics (for example a large part was not aware that providing access to data and viewing the data also constitutes processing). On a positive note, the processors were generally cautious when processing.
- [46]. There has also been an internet campaign regarding the activities of children on the Internet.<sup>13</sup> The website, which was created in cooperation by the *Lastekaitse Liit* [the Estonian Union for Child Welfare] and EDPI, informs children and young people, parents and teachers of the potential dangers and threats faced by children online. There has also been a more general outdoor media campaign highlighting the issue of identity theft.
- [47]. The EDPI plans to conduct a new survey in 2009.<sup>14</sup> Other surveys conducted in the area of fundamental rights have not specifically covered data protection. The survey will provide valuable data on whether the situation has improved.
- [48]. The EDPI also plans to continue to raise awareness, in particular through media. This is done mostly by publishing articles written by

---

<sup>12</sup> *Turu-uuringute AS* (12.2006) *Elanikkonna ja asutuste teadlikkus isikuandmete kaitsmisest* [Population's and Institutions' Awareness of Personal Data Protection], available at: <http://www.aki.ee/document.php?id=115> (23.01.2009).

<sup>13</sup> See: <http://www.peremeedia.ee/> (29.01.2009).

<sup>14</sup> Estonia/Andmekaitse Inspektsioon (01.04.2008) *Andmekaitse Inspektsiooni ettekanne 01. jaanuar 2007-31. detsember 2007* [Report of the Estonian Data Protection Inspectorate 1 January 2007-31 December 2007], available at: <http://www.aki.ee/est/systematic/files.php?id=696> (23.01.2009).

the officials of the EDPI. Special attention was given in 2008 to the processing of personal data at educational institutions, and in 2007 to pharmacies and medical service providers.<sup>15</sup>

---

<sup>15</sup> Estonia/*Andmekaitse Inspeksioon* (01.04.2008) *Andmekaitse Inspeksiooni ettekanne 01. jaanuar 2007-31. detsember 2007* [Report of the Estonian Data Protection Inspectorate 1 January 2007-31 December 2007], available at: <http://www.aki.ee/est/systematic/files.php?id=696> (23.01.2009), pg 52.



## 6. Analysis of deficiencies

- [49]. From a fundamental rights perspective there are no major deficiencies regarding effective data protection and effective relevant institutions in Estonia. The issues that were present in the former iterations of law regarding confusion between private and sensitive personal data, as well as other issues, have now been solved. The PDPA brought Estonia into full compliance with Directive 95/46/EC.
- [50]. One of the main issues is the relative lack of knowledge among the public regarding the rights and obligations related to data processing. The EDPI should do more to popularise and raise awareness about the specific principles of data protection, both among the population in general, but also in specific sectors.
- [51]. There are a number of sectors in which it seems that the data protection rules have yet to be followed. In an interview with the daily newspaper *Postimees*, the new Director General of the EDPI stated that in about 80% of municipalities and local governments, data protection rules are not followed, and alternative registries of inhabitants are being kept.<sup>16</sup>
- [52]. No major areas are automatically excluded from the data protection law. The law does not apply to processing by a natural person for personal use nor to the transmission of personal data through the territory of Estonia without processing (§ 1 of the PDPA). There are also specific exemptions for criminal and court proceedings. In a criminal procedure, information gathered during pre-trial proceedings can be published only where it does not cause harm to the data subject, in particular in relation to sensitive personal data (§ 214 (2) p 4 of the *Kriminaalmenetluse seadustik* [Code of Criminal Procedure]).<sup>17</sup>
- [53]. The publication of information gathered during investigations is a matter that has created significant public debate because in several high-profile cases, transcripts of secretly recorded phone calls, SMS messages and other information, which also may contain sensitive personal data, has leaked from either the prosecutors or defendants' attorneys. The *rüigiprokuratuur* [State Prosecutor's Office] has suggested to the *justiitsministeerium* [Ministry of Justice] that it prepare an amendment of the criminal procedure regulations in such a way as to limit the access of defence attorneys to the materials

---

<sup>16</sup> A. Lõhmus (2008) 'Andmekaitse uus juht näeb rahvastikuregistris suuri läbivaid vigu', in: *Postimees.ee* (24.10.2008), available at: <http://www.postimees.ee/?id=43265> (29.01.2009).

<sup>17</sup> Estonia/*Riigikantselei* (2003) *Riigi Teataja* [State Gazette] I, 27, 166.

included in the court files.<sup>18</sup> However, the suggestion received a negative response both from the Minister of Justice and the *Eesti Advokatuur* [Estonian Bar Association], as the access to documents for the defendant is an important guarantee of the right to a fair trial.

- [54]. The legislation seems to be in place and well in line with international and EU standards, however awareness needs to be raised further. The forthcoming survey on the awareness of data protection rules should provide more information as to whether or not awareness has improved and which measures should be implemented.

---

<sup>18</sup> Estonia/*Riigiprokuratuur* [State Prosecutor's Office] (17.12.2008) *Prokuratuur soovib piirata kaitsjatele antavat materjali* [The State Prosecutor's Office wishes to restrict materials given to defence], available at: <http://www.prokuratuur.ee/39806> (29.01.2009).

## 7. Good Practice

- [55]. The wide range of advisory guidelines published by the EDPI should be noted as providing the basis for good practice. The EDPI has published in total 24 sets of guidelines.<sup>19</sup> These include an article related to the processing of personal data and registration requirements in schools,<sup>20</sup> Guidelines on the Registration of Processing of Delicate Personal Data by Security Companies,<sup>21</sup> Guidelines on Issuing Customer Loyalty Cards,<sup>22</sup> Guidelines on the Publication of Donors to Political Parties,<sup>23</sup> Guidelines on Taking Photos at Pre-School Institutions,<sup>24</sup> Guidelines on Processing Personal Data in Accommodation Establishments,<sup>25</sup> and Guidelines on the Processing of Flight Passenger Records.<sup>26</sup>
- [56]. Another example of good practice is the ability to submit complaints electronically by using digitally signed documents.<sup>27</sup> This is a part of the government-wide e-services push and the process for submitting a complaint is relatively straight-forward. The EDPI has made available on its website the requirements for submitting the written complaint, which must include the name of the complainant, the content of the complaint, the date, a signature and contact details. In order to send the document by e-mail, it has to be digitally signed for which a person needs a working computer, ID-card reader and the Estonian ID-card with appropriate pin-codes.<sup>28</sup>

---

<sup>19</sup> See: <http://www.aki.ee/est/?part=html&id=56> (23.01.2009).

<sup>20</sup> U.Kukk (2008) 'Dokumentatsioon korda!', in *Õpetajate Leht nr 19* (16.05.2008).

<sup>21</sup> Estonia/*Andmekaitse Inspeksioon* (2.06.2008) *Turvaettevõtete poolne delikaatsete isikuandmete töötlemise registreerimine* [Guidelines on the Registration of Processing of Delicate Personal Data by Security Companies], available at: <http://www.dp.gov.ee/document.php?id=733> (21.10.2008).

<sup>22</sup> Estonia/*Andmekaitse Inspeksioon* (07.01.2008) *Isikuandmete koosseis kliendikaardi väljastamisel* [Guidelines on Issuing Customer Loyalty Cards], available at: <http://www.dp.gov.ee/document.php?id=592> (21.10.2008).

<sup>23</sup> Estonia/*Andmekaitse Inspeksioon* (10.03.2008) *Erakondade rahastajate isikuandmete avalikustamine* [Guidelines on the Publication of Donors to Political Parties], available at: <http://www.dp.gov.ee/document.php?id=661> (21.10.2008).

<sup>24</sup> Estonia/*Andmekaitse Inspeksioon* (10.03.2008) *Pildistamine koolieelsetes lasteasutustes* [Guidelines on Taking Photos at Pre-School Institutions], available at: <http://www.dp.gov.ee/document.php?id=662> (21.10.2008).

<sup>25</sup> Estonia/*Andmekaitse Inspeksioon* (3.04.2008) *Isikuandmete töötlemine majutuseettevõtetes* [Guidelines on Processing Personal Data in Accommodation Establishments], available at: <http://www.dp.gov.ee/document.php?id=698> (21.10.2008).

<sup>26</sup> Estonia/*Andmekaitse Inspeksioon* (22.04.2008) *Lennureisijate andmete töötlemine* [Guidelines on the Processing of Flight Passenger Records], available at: <http://www.dp.gov.ee/document.php?id=705> (21.10.2008).

<sup>27</sup> See: <http://www.aki.ee/est/?part=html&id=55> (23.01.2009).

<sup>28</sup> See: <http://www.aki.ee/est/?part=html&id=55> (29.01.2009).

- [57]. As the data protection legislation is relatively new, there are no major courts cases or practices to report that have brought about significant new developments, but for the *Hansapank* case. Other noteworthy cases have not resulted in any formal decisions and the other cases reported in the Annex are indicative of the kind of cases handled.

## 8. Conclusions

- [58]. The protection of personal data is well regulated in Estonia and there are no major deficiencies in the law itself. The Estonian Data Protection Inspectorate is well equipped to handle the data protection rules and it has been working effectively. It actively provides information on the data protection rules and has issued numerous advisory guidelines for data processors and data subjects.
- [59]. There are a few areas of concern. The EDPI also monitors the fulfilment of the Public Information Act, therefore these dual functions may sometimes lead to contradictory situations within the sphere of governmental institutions because the EDPI may be required to balance simultaneously two very different rights: the right of the public for access the public documents and at the same time the right for potential data subjects for the protection of personal data. This may also have an impact on the allocation of resources for the data protection side of the activities of the EDPI.
- [60]. The other concern relates to the selection process of the Director General of the EDPI, which might undermine the independence of the EDPI. As a head of an independent institution, which should also oversee the activities of other governmental bodies, the transparency of the selection process is particularly important.
- [61]. The sanctions are adequate, notably following the introduction of criminal sanctions in 2007, and the fines for legal persons were increased to a maximum of 500 000 *kroons*. However, as the data protection legislation has rarely been tested in court, it is unclear how willing the courts are in providing specific compensation and whether they also offer compensation when no monetary damages have been received.
- [62]. For the protection of personal data, as well as human rights in general, awareness is low. Although people in general are aware of the existence of the rights and obligations, they are unable to furnish these with specific content.
- [63]. The EDPI is proactive in raising awareness and rather than trying to punish and sanction in specific cases, it tries to educate and assist in remedying the deficiencies. This is useful in this early stage where awareness of the legal requirements of data protection is low, but at some point there needs to be tougher actions. The area-specific approach by the EDPI, by focusing on specific areas in which awareness is low, is also helpful.

- [64]. The numerous advisory guidelines, which explain in detail the application of data protection for specific target groups are especially helpful. The EDPI publishes these guidelines as a reaction to an issue which has arisen within the media or on its own initiative.

# Annexes

## Annex 1 - Tables and Statistics

Please complete the table below

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority in million EEK	3,56	4,77	4,40	4,61	4,81	6,79	7,92	8,85
Staff of data protection authority	15	18	17	17	18	16	23	20
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	N/A	N/A	N/A	16	8	8	30	77
Number of data protection registrations (requests for registration)	N/A	N/A	N/A	497	464	368	456	629

Number of data protection approval procedures	36	235	372	289	314	361	351	644
Number of complaints received by data protection authority	N/A	N/A	N/A	98	27	41	37	46
Number of complaints upheld by data protection authority	N/A	N/A	N/A	0	0	11	15	6
Follow up activities of data protection authority, once problems were established (precepts/fines).	N/A	N/A	116/-	50/14	35/5	18/8	33/15	96/4
Sanctions and/or compensation payments in data protection cases in EEK.	N/A	N/A	8 000	10 000	73 700	35 600	79 150	8 400
Range of sanctions and/or compensation in your country (administrative fine for private individual / administrative fine for legal person / criminal sanctions)	N/A	N/A	N/A	18 000 / 50 000	18 000 / 50 000	18 000 / 50 000	18 000 / 50 000	18 000 / 500 000 / monetary punishment or up to one-year imprisonment
Court cases under the PDPA	N/A	N/A	0	0	0	1	0	1



## Annex 2 – Case Law

There is no case-law available in the courts. There are additional decisions based on complaints to the EDPI, but these provide no value for the purposes of this study.

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

<b>Case title</b>	Complaint of AS Hansapank to repeal the precept no 2.1-9/06/19 of the Estonian Data Protection Inspectorate from 30 November 2006
<b>Decision date</b>	16 June 2008
<b>Reference details</b> (reference number; type and title of court/body; in original language and English [official translation, if available])	Case no 3-07-317, Tallinna Ringkonnakohus [Tallinn Court of Appeal], court of second instance
<b>Key facts of the case</b> (max. 500 chars)	Mr Roster repeatedly breached the obligation to repay the debt taken with a deferred debit card issued by AS Hansapank and therefore Hansapank published the debts in the credit register of the public website of AS Krediidinfo in June 2001. The debtor repaid the debt in April 2006 and filed a complaint in September 2006 with the EDPI for the publication of his personal data on the Krediidinfo site, as he had not given consent for this and had repaid the debt. The EDPI issued a precept which required AS Hansapank to stop processing by 11 December 2006, which the bank contested in court.
<b>Main reasoning/argumentation</b> (max. 500 chars)	The bank had failed to obtain Mr Roster's consent to the publication of personal data at the Krediidinfo site (transmitting the data to a third party). It also had failed to specify the purposes of data processing in the contract signed with Mr Roster.
<b>Key issues (concepts, interpretations) clarified by the case</b> (max. 500 chars)	This was one of the first cases applying the new PDPA, it also clarified the legal status of credit information websites and the obligations of the bank.
<b>Results (sanctions) and key consequences or implications of the case</b> (max. 500 chars)	The Court upheld the precept, which ordered the termination of the processing of personal data. The commercial banks now need to obtain express consent for the processing of data in their credit agreements, including the purposes, in order to publish such information in a public credit register.

<b>Proposal of key words for data base</b>	Public credit register, unauthorised transmission to third parties, banking sector.
--------------------------------------------	-------------------------------------------------------------------------------------

<b>Case title</b>	Claim by M.K. and M.S. against <i>Tartu Kesklinna Perearstikeskus</i> and L.L. to correct the incorrect information on the health card and for the compensation of moral damages.
<b>Decision date</b>	7 March 2008
<b>Reference details</b> (reference number; type and title of court/body; in original language and English [official translation, if available])	Case no 2-07-49130, Tartu Ringkonnakohus [Tartu Court of Appeal], court of second instance, appeal against court ruling
<b>Key facts of the case</b> (max. 500 chars)	The claimants filed a suit against the defendants to correct incorrect information in the health card, which was put there without an examination being made of the patient by the family doctor. Tartu County Court refused to hear the case.
<b>Main reasoning/argumentation</b> (max. 500 chars)	The Tartu County Court claimed that it was not a competent authority to hear the case because it concerns sensitive personal data, thus the EDPI is the competent supervisory authority to whom the complaint should be filed. The Appeals court did not agree with the County Court.
<b>Key issues (concepts, interpretations) clarified by the case</b> (max. 500 chars)	The case clarified the remit of the EDPI with regard to medical data and the specific obligation placed on medical service providers with the Law of Obligations Act.
<b>Results (sanctions) and key consequences or implications of the case</b> (max. 500 chars)	The Appeals court overturned the decision and sent the case back to the County Court for hearing as it classified the dispute as falling under Law of Obligations Act.

<b>Proposal of key words for data base</b>	Supervision of medical services, remit of data protection authority.
--------------------------------------------	----------------------------------------------------------------------

<b>Case title</b>	Precept to Tallinn Central Library
<b>Decision date</b>	18 January 2008
<b>Reference details</b> (reference number; type and title of court/body; in original language and English [official translation, if available])	Precept of the Estonian Data Protection Inspectorate to Tallinn Central Library
<b>Key facts of the case</b> (max. 500 chars)	The case concerned the electronic entry system of the library which displayed the name of the five last customers passing through the entry gate on the small screen next to the gate. This information was visible to all visitors to the library.
<b>Main reasoning/argumentation</b> (max. 500 chars)	The publishing of the name of the customers passing through the library gate was considered unauthorised publication of personal data by the EDPI and was required to be stopped.
<b>Key issues (concepts, interpretations) clarified by the case</b> (max. 500 chars)	Whether publication of a log of names of people passing through an electronic gate is allowed.
<b>Results (sanctions) and key consequences or implications of the case</b> (max. 500 chars)	The precept was fulfilled by the library and the system was modified. The case was publicised in the media.
<b>Proposal of key words for data base</b>	Access system, publication of name log.