Data Protection Inspectorate

A report on the observation of the Personal Data Protection Act and Public Information Act

2005

Tallinn 2005

The Data Protection Inspectorate presents the report to the Constitutional Committee of the Riigikogu and to the Chancellor of Justice on the basis of § 41 (1) of the Personal Data Protection Act[1] and § 54 (1) of the Public Information Act[2] on the circumstances derived from the observation and application of the aforementioned Acts.

The area of activity of the Inspectorate is state surveillance of the processing of personal data, management of databases and access to public information and also the discharge of functions set by other Acts or legislation.

The report was compiled by: Gina Kilumets (director of the research and analysis department), Maarja Kirss (adviser of the research and analysis department), Rainer Kivisäk (director of the registration division fulfilling the obligations of the director of the control department) and Bert Blös (deputy of the director of the proceedings division).

1 SG I 2003.26.158; 2004.30.208
2 SG I 2000.92.597; 2002.61.375; 63.387; 2003.25.153; 26.158; 2004.81.542

Introduction

The Constitution[3] of the Republic of Estonia states the right for privacy, right to privately exchange information and the right for data protection. § 42 of the Constitution states that state authorities, local governments and their officials are not allowed to gather or save information about the beliefs of the citizens of Estonia, § 43 states, that each and everyone has a right for secrecy concerning messages transmitted to him via post, telegraph, telephone or other means generally in use. Exceptions can be made with a decision from the court for determining the truth in criminal proceedings according to the laws and legislation in force. Subsection 1 of Section 44 states that all state authorities, local governments and their officials are obliged to provide the citizens of the Republic of Estonia information concerning their activities as described in the law, except information, which cannot be disclosed on account of the law, and information, which is exclusively for in-house usage. Subsection 2 of the same paragraph states that Estonian citizens have the right to access information about them that is stored in state authorities and local governments, also at state and local archives.

The main aim of the Data Protection Inspectorate (henceforth DPI), which is in the jurisdiction of the Ministry of Internal Affairs, is the protection of fundamental rights and freedoms of citizens in processing personal data and the persons' right for fundamental information.

The increase in public awareness about the extent and legislation of personal data processing was largely achieved by constant public attention and frequent media coverage of the subject. Nevertheless, there are still two problematic issues in applying personal data processing requirements: the legality of data processing and providing the required safety during processing. In addition to personal data protection, the DPI also maintains surveillance over public knowledge. Taking into account the events of the last year and their coverage in the media, data disclosure is a relevant topic at the moment.

The report at hand is the fifth concerning the observation of the Public Information Act (PIA) and the third concerning the observation of the Personal Data Protection Act (PDPA). The report gives an overview of the most important facts and events of 2005 concerning public information and personal data protection and also provides information on plans and projects for the next year.

The budgetary resources of the inspectorate for 2005 were 6 851 473 croons. The Inspectorate has 31 employees, and as of November 30, 2005, the inspectorate has appointed 6 employees. 14,5 positions are filled (three employees at 0,5 work load). The inspectorate has no junior officials, support staff or non-staff officials. The DPI structure is comprised of three departments: development and analysis department, control department and administrative department.

DPIs' planning for cost-saving and increasing effectiveness has been optimised to the maximum in the recent years. The inspectorate has been working with a limited capacity over the recent years, meaning that both human and financial resources have been utilized to the maximum: during the last two years, the work-load of the

3 SG I 1992.26.349; 2003.29.174; 64.429

Inspectorate has increased with the application of different laws, but neither the budget nor human resources have increased. In conjunction with the increase in budget for 2005, the Inspectorate planned for 5 new employees, but during the report year three employees left for other state authorities. The situation is problematic, as instead of hiring new staff according to the initial plan, the inspectorate has to deal with replacing staff. The positions of the officials who left the inspectorate must be filled. As the officials of the inspectorate are suitable for other state authorities thanks to their acquired know-how, the acquiring of staff by other state authorities has become increasingly frequent (three times by other state authorities during 2005).

Surveillance over the processing of personal data

During the period from December 1, 2004 until November 30, 2005, 368 applications for processing sensitive personal data were presented, of which 61 were returned and 29 were refused. As of November 30, 2005, 1550 processors have registered the processing of sensitive personal data.

Concerning the applications, the most notable thing is the decrease in submitted applications, but, on the other hand, the sophistication and the capacity of the application have gone up. The number of applications for registering the processing of sensitive personal data by the public sector has increased. Compared to other period, the number of rejections has decreased dramatically, which indicates the rise in the quality of applications for processing of sensitive personal data, or in other words the awareness of processors (concerning both data processing and formalizing of documents).

The most prominent registrars were: Border Guard Administration, Prosecutor's Office, different registries and data collection projects of the Ministry of Social Affairs, Statistical Office, Ministry of Justice (criminal proceedings register), Labour Inspectorate, Competition Board, Harju County Government, State Archives, Ministry of Internal Affairs, State Audit Office, Tax and Customs Board, Health Protection Inspectorate, Ministry of Education and Research, Ministry of Defence etc.

The compliance of various organizational, physical and information technological protection measures applied by processors of sensitive personal data with the requirements of the PDPA were checked on 535 occasions (it must be taken into account that during the processing of one application, the surveillance division can provide a different response during the different stages of the process: return of application, registration or denial of registration of the application etc.). Local inspection was carried out 28 times (2004: 35; 2003: 49; 2002: 77; 2001: 135), of which on 8 occasions the posterior control was done on self-initiative and on 3 occasions the concordance with precepts were checked. The lack of inspections is due the lack of staff. The processors were issued with precepts on 4 occasions and cautioned on 5 occasions.

The DPI received 41 complaints concerning to the PDPA, of which 11 were founded. Most of the identified infringements were related to granting access to personal data of data subjects or this information was transmitted to third parties without legal grounds, which in civil matters can only be provided by the data subject and public matters by an authorization in accordance with the law. Despite the fact that in some of the identified cases the personal data of the data subject was disclosed to an unlimited number of third parties via the Internet, the personal data was so-called ordinary personal data (name of person, e-mail address etc.) of only one or a small number of data subjects. The only distinction that has to be made when dealing with the abovementioned infringements is the difference between human error and lack of knowledge. When dealing with the aforementioned, the processors reacted quickly and rectified the shortcomings, in the second case, the processors were not aware of their infringement and for the protection of the rights of the data subject they were issued with precepts. In total, the Inspectorate issued 4 precepts and initiated 5 misdemeanours towards the employees during the reporting period, of which 2 are

resolved and 3 are still being processed. In both of the resolved cases the cause was the lack of regard toward requirements, which consisted of transferring personal information of the data subject without legal grounds or allowing third parties to access such information.

According to § 14 (2) of the PDPA, transferring of personal data or allowing third parties to access personal data without the permission of the data subject is allowed on three occasions:
1) if the person who is the recipient of the data processes them for fulfilling obligations set upon him or her in the law;

2) if the transferral of data is required for the protection, health or freedom of the data subject or any other person;

3) if the third party applies for the data, which is gathered or created by the law or according to the legislation for public purposes and no access restrictions have been set upon such data.

On both occasions, personal data with access restrictions were transferred, in the first case from the state traffic register and from the border crossings database.

Therefore transferring such personal data or allowing access to such personal data is only allowed on conditions 1 and two from the aforementioned list. On both of the occasions the third party was not processing them for fulfilling obligations set upon him or her in the law. Also, the personal data transferring or allowing access to such personal data was not done to protect the health, life or freedom of the data subject or any other person.

The remaining three initiated misdemeanour processes are most probably related to failures to meet the obligations set in § 6 (19) of the PDPA, obligation to employ organizational, physical and information technological protective measures for the protection of personal data. A processor authorized and responsible for personal data is, among other things, obliged to ensure that during the transport or transfer of personal data the personal data is not read, copied, altered or deleted during transit. In the first case, the data carriers used for transport of personal data which left the possession of the personal responsible for them or the processor, enabling the data to be read, copied, altered or deleted were approximately 100 expired health insurance cards, in the second case approximately 400 sick leave certificates of patients of a gynaecologists and in the third case a memory card with the names and addresses of approximately 300 000 persons liable to serve in the Defence Forces.

The Data Protection Inspectorate received 32 clarification applications related with personal data protection. The officials of the Inspectorate have carried out over 30 different training programs regarding personal data processing requirements and personal data disclosure. State or local government departments ordered approximately 85% of the ordered training programs.

Problem cases of 2005:

The Ministry of Social Affairs and the register for communicable diseases
The dispute concerning the register for communicable diseases and the composition of the gathered data arouse already in 2004 with the Ministry of Social Affairs. The DPIs' assessment stated that the composition of gathered data surpassed the delegacy norms (according the Communicable Diseases Prevention and Control Act[4] it was only permissible to gather personal data related with epidemic and extremely dangerous communicable diseases).

According to established order, personal data is gathered and stored (for 75 years) about, among other diseases, scabies and animal bites etc. or in other words, about diseases which do not qualify as extremely dangerous communicable diseases or as epidemic communicable diseases. The Ministry of Social Affairs has, among other things, substantiated the gathering of personal data with the war on terrorism, and also that the spreading of all communicable diseases listed in regulation no. 297 "Procedure for disclosure of information concerning the appearance of and sickening in communicable diseases and the composition of information to be disclosed"[5] have same outcome – epidemic, massive sickening of the population and high mortality rate of both adults and children.

The Data Protection Inspectorate also addressed the Government of the Republic with the question, as a result of which the Ministry of Social Affairs admitted the existence of the problem by summer 2005 and the conflict between the applicable legislation and the law.

On the initiative of the Ministry of Social Affairs, the Communicable Diseases Prevention and Control Act was amended and the delegacy norm was added for the Government of the Republic to establish the communicable disease list which states the cases when it is allowed to present personal data to the registry. The implementing provision has not been accepted yet.

The state register for communicable diseases was created on January 1, 2005 on the basis of the Health Protection Inspectorate's departmental register, meaning that the existent database was given the status of state register. The controller of the register is the Ministry of Social Affairs and the processor the Health Protection inspectorate. Regulation no. 377 "Usage of the state register of communicable diseases and management of registry statutes"[6] states that the register is maintained digitally. Until this moment, registry management was done only on paper and as the controller and the processor have chosen software (Excel, member of the MS Office package) that is unsuitable for managing the database, the provisions of the Personal Data Protection Act have not been met. With the directive from the Health Protection Inspectorate, the Health Protection Inspectorates' communicable disease register was created in 2005, which replicates in full the state register, uses the same source documents etc. Taking into account the Database Act, which forbids the management of duplicate registers, the Data Protection Inspectorate approached the Ministry of Social Affairs with a recommendation to have the establishment directive of the aforementioned register

4 SG I 2003.26.160; 2004.27.177; 30.208; 2005 13.63; 24.180
5 SG I 2003.76.512
6 SG I 2004.91.629

nullified. The Ministry of Social Affairs is still processing the recommendation.

Tuberculosis record
A question has arisen in connection with the tuberculosis record regarding the management of databases created on the basis of § 8 (1.12) of the Public Health Act[7]. The aforementioned article states that the objective of the Ministry of Social Affairs is to gather data related to the health of the population and process personal data for the developing and implementing, in accordance with the Personal Data Protection Act and Public Information Act, the state health and healthcare policy.

Practically this means that the Ministry of Social Affairs has been given the authority to determine the basis and conditions of limitation of fundamental rights and freedoms, therefore the right to decide which personal data, and to what extent, is gathered about the data subject.

Based on the aforementioned provision delegating authority, various databases have been created: birth record, tuberculosis record etc. All such records require the clients of healthcare services to provide miscellaneous statistical information (for instance: place of birth; education; field of activity, lifestyle, job etc.)

According to § 764 of the Law of Obligations Act[8] the patient is obliged to provide the healthcare service provider all the required information he or she deems necessary for providing a healthcare service and, if necessary, assist the healthcare service provider in any way possible.

It is incomprehensible why the healthcare service provider is obliged to gather and present the aforementioned personal data about the patient. According to applicable regulations, it is unclear whether the patient is or is not obliged to provide such data and whether not providing such data affects the healthcare service being provided for the data subject. In pursuance of § 51^1 of the Database Act[9], a legal person can be fined up to 30 000 croons for failure to present mandatory personal data to state or local government databases or for providing false information to state or local government databases.

In conclusion, a situation has been created where, by the regulation of the Ministry of Social Affairs, the healthcare service provider is obliged to present personal data about the patient which the is not obliged to provide and failure to provide such data by the health care service provider is liable to prosecution.

Statistical office and cancer record
The attempt by the Statistical office to use data gathered during a state statistical survey for complementing other state records.

The Statistical office and Põhja-Eesti Regionaalhaigla foundation signed a contract in summer 2005, which states that the executor of the contract (Põhja-Eesti

7 SG I 1995.57.978; 1996.3.56; 49.953; 1997.37/38.569; 1999.30.415; 88.804; 2001.23.128; 2002.32.187; 53.336; 61.375; 63.387; 90.251; 2003.26.156; 26.160; 2004.45.315; 75.520; 87.593
8 SG I 2001.81.487; 2002.53.336; 60.374; 2003.78.523; 2004.13.86; 37.255; 75.522; 87.593; 90.616
9 SG I 1997.28.423; 1998.36/37.552; 1999.10.155; 2000.50.317; 57.373; 92.597; 2001.7.17; 17.77; 2002.61.375; 63.387; 2003.18.107; 26.158; 2004.30.204

Regionaalhaigla) checks, marks and complements personal data entries in the cancer records, which match the data file descriptions of the signatory (The Statistical office)

The cancer record is a database created by the Ministry of Social Affairs, which, in the meaning of the Database Act, is an 'other database'. The controller of the cancer record is the Ministry of Social Affairs and the processor is Põhja-Eesti Regionaalhaigla.

According to § 8 (2) of the Official Statistics Act (henceforth OSA)[10], the data gathered on a state statistical survey can be used only for statistical purposes. Section 3 of the same Article states that data gathered on s state statistical survey cannot be used for inspection, taxation or any other non-statistical function.

Based on the evaluation of the Statistics office, the complementation of the cancer record with data gathered during state surveys permissible and also necessary for ensuring the fullness and quality of the state cancer statistics, which can only be achieved by bilateral supplementation of data. At that, the Statistics office was unable the unable to answer the question of the Data Protection Inspectorate: for which state surveys is it allowed to supplement the information in databases managed by reporting agents gathered from state surveys for the fullness and quality of the state statistical surveys and on which legal Acts does the Statistics office base its decision on.
By this moment, the Statistics office has ceased its activities of this nature.

Taxable persons record
The attempt by the Statistics office to take over the taxable persons record in full.

The taxable persons record is a state record and its controller and processor is the Tax and Customs Board. Based on the evaluation of the Statistics office, the Statistics office requires 95% of the full content of the taxable persons record twice per month and in the form, which includes personal data. The Statistics office bases its claim on § 7 (2) of the OSA, which states that state and local governments are obliged to present data, which has been collected through their own activities, to the organizer of the state and statistical surveys on their request.

At this point, the Statistics office has failed to notice that, according to the Official Statistics Act, the reporting agent is obliged to only present personal data in the extent set in the yearly state statistical survey list issued by the Government of the Republic. (§ 3 (2,3) and § 7 of the OSA). In addition to that, the Statistics office considers it permissible to request personal data for such surveys, which, according to the state statistical surveys list, are to be done without personal data.

Based on the example in question, the Tax and Customs Board is the reporting agent for different state statistical surveys. These surveys in general state the need for consolidated data, meaning that the submitted data does not enable the data subject to be identified.

Procuring of personal data from the Tax and Customs Board is only for inspection of data about persons who participated in a social survey. 5000 data subjects will be

10 SG I 1997.51.822; 2000.47.289; 2002.63.387; 2004.30.204

involved in this survey. Based on the assessment of the Statistics office, the Tax and Customs Board is obliged to present the taxable persons record in the extent of 95%, after which the Statistics office is to decide which data is used for which survey and which data the survey would, in reality, require.

Based on the assessment of the Data Protection Inspectorate, such a request by the Statistics office is unfounded and in violation with the Personal Data Protection Act and also the Official Statistics Act. The dispute in this matter is nearly closed.

The described situation, once again, confirms the need for detailed reasoning and limitations in carrying out yearly state statistical surveys in order to prevent a situation where, due to the misinterpretation by an administrative office, the privacy of hundreds of thousands individuals is at risk.

Record of the healthcare service provider
A digital database, created by one of the largest healthcare service provider, used all over Estonia by different healthcare service providers, does not meet the provisions of the law. The Data Protection Inspectorate detected the aforementioned fact during surveillance procedures. The creators or the users had not informed the Data Protection Inspectorate of the existence of such an database, thus violating the requirement set in the Personal Data Protection Act stating the need for registering alterations.

In this case, the healthcare service providers are controllers of personal data, who authorized the processing of certain data for the owner of the database. The problem with the usage of the database in question is that the sensitive personal data of data subjects added to the database is accessible to all parties who have joined the system (healthcare service providers) and for research work (the controller and processor of personal data are obliged to ensure that each user of the data processing system has access only to the personal data of the data subject he or she is authorized to access and authorized to process). In addition to that, the data subjects were not informed that their personal data was accessible to all healthcare service providers using the same service, which also meant that the activities were carried out without the consent of the data subject.

The Data Protection Inspectorate presented the creator of the database with a precept obliging the latter of ensuring the requirements of the Personal Data Protection Act are met and, at this stage, the dispute is close to being resolved.

Surveillance over the observation of the Public Information Act

During the report period, the DPI received 40 challenges concerning violation of the rights set forth in the Public Information Act. Of the 40 challenges, 13 were returned and 27 were accepted for processing. The main reason behind returning challenges was the fact that the different appeals for the holders of information were not requests for information in the sense of requests for recorded or documented information, but clarification requests, which requires the analysis, synthesis of the recorded or documented information or requires the gathering of additional knowledge. It became apparent during the process that the holders of information were in breach of the law on approximately half of the occasions. When answering clarification requests, the Public Information Act is not applied.

In some violation cases, the legality was restored during the process and in which cases the challenge of the challenger was dissatisfied and on 9 occasions the challenge of the challenger was satisfied and the holder of the information was presented with a precept.

The average penalty payment set in the precepts was 10 000 croons, which in general is sufficient to guide the holder of information to uphold the law.

The main violations were failures to uphold deadlines; failures to meet the obligation of public disclosure or in other words, failure to disclose information on web pages; wrongful interpretation of the Public Information Act and establishment on illegal access limitations and unjustifiable refusals to satisfy requests for information.

The most important violations of the Public Information Act:

Äripäev and Ida-Tallinna Keskhaigla
Äripäeva Kirjastuse AS presented the Ida-Tallinna Keskhaigla with a request for information requesting the commercial lease contracts for hospital rooms for the year 2004. The hospital refused the request for information claiming that by commercially leasing the hospital rooms the hospital acts as a legal person governed by private law and realises its right of ownership and that it is not providing a public service, which, for a hospital, is providing healthcare services. During the process, Ida-Tallinna Keskhaigla AS was explained that, in some cases, the obligations of holders of information also apply for legal persons governed by private law. Mainly because if the state or local government or any legal person governed by public law is a participant in founding or is a participant in a non-profit organization, foundation or a company and concerning information, which concerns the usage of resources allocated from the state or local government's budget for the legal person governed by public law. The holder of information cannot declare such information as internal.

AS Ida-Tallinna Keskhaigla was founded based on decision no. 226 of the Tallinn City Council on the 23rd of August 2001, by merging Tallinn Magdaleena Hospital, Tallinn Central Hospital, Tallinn Nursing Hospital, Tallinn Järve Hospital, Tallinn Tõnismägi Polyclinic and Tallinn Mäekalda Polyclinic. Based on the information of the commercial register, the founder and sole shareholder of AS Ida-Tallinna Keskhaigla is the city of Tallinn. Therefore the obligations of a holder of information apply to the Ida-Tallinna Keskhaigla AS as a legal person governed by public law,

including the restriction to declare information internal, which deals with the budget and other assets allocated from the budget of the local government.

According to the city of Tallinn, the leasing out of buildings and lease contracts of Ida-Tallinna Keskhaigla AS is to be considered as information, which deals with exploitation of assets provided by to a company founded by an unit of the local government.

The holder of information admitted that different buildings have been handed over to Ida-Tallinna Keskhaigla AS for public usage and decided to satisfy the request of the person making the request for information and to disclose the requested information.

Lohusuu Rural Municipality Government
A citizen presented the Lohusuu Rural Municipality Government with a request for information, which contained the request for the disclosure of the certified project documentation for the building that is constructed on a neighbouring registered immovable. The rural municipality government refuses to accept the request for information on the grounds of a tense and intense time schedule, requirement for the inviolability of life and the absence of the permission of the author of the project. All these grounds were found unfounded

The issuing of a construction permit is done partly on the basis of the Building Act[11] and partly on the basis of the Administrative Procedure Act[12] (henceforth APA). Construction and planning action is public and in pursuance of § 7 (1) of the APA the administrative proceedings are public. Pursuant of § 18 (1) of the Building Act, the construction project is a required collection for the construction and exploitation of a building and is comprised of figures, explanatory letter and instructions on maintenance and of other relevant documents.

In this case, the project documentation for the building being constructed on the basis of construction permit no. 102036690 contained no personal data in the sense of the Personal Data Protection Act, as there were no references made to specific natural persons – data subjects. Also, the planned construction was not for a private residence, but for accommodations.

Therefore the basis – ensuring the inviolability of life – of the holder of the information for refusal to disclose information was unfounded. The reference by the holder of information to the absence of the permission of the author of the project was appropriate, but not legitimate. According to § 19 (8) of the Copyright Act[13], reproduction of a work is permitted without the necessity to pay remuneration, but with the obligation to display the name of the author and if the work includes, then the title and primary source of the work and for the administration of justice or during administrative processes or for ensuring public security to the extent which meets the needs of the administration of justice or administrative purposes for ensuring public security.

11 SG I 2002.47.297; 99.579; 2003.25.153; 2004.18.131
12 SG I 2001.58.354; 2002.53.336; 61.375; 2003.20.117; 78.527
13 SG I 1992.49.615; 1996.49.953; 1998.36/37.552; 1999.10.156;29.398; 36.469; 97.859; 2000.13.94; 16.109; 78.497; 2001.50.289; 56.335; 2002.53.336; 63.387; 90.521; 92.527; 2004.18.131; 30.208; 71.500; 77.527; 2005.37.287

The issuing of a construction permit is an administrative process of the rural municipality and the building design document is the basis for issuing a construction permit. With regard to the aim of the PIA, which is to provide opportunities for the inspection of publicity during the fulfilment of public duties on the assumption of democratic and social rule of law and public principles of society, the disclosure of the building design document copies without the approval of the author on the basis of the request for information is in concordance with the Copyright Act. Moreover, the Estonian legal system the issuing of a construction permit is the inspection of legalism and it is to be done by the public.
The holder of information acted in concordance with the Public Information Act in dealing with the information request.

OÜ Siromets and East Police Prefecture
OÜ Siromets presented the Rakvere Police Department, East Police Prefecture, with a request for information requesting the disclosure of a misdemeanour decision and misdemeanour protocol of a certain misdemeanour process. The misdemeanour concerned was a traffic accident with a motorcar leased by OÜ Siromets. The handler of the information refused to satisfy the request for information and based the refusal on § 14 (5) of the Code of Misdemeanour Procedure[14] and the circumstance that the person making a request for information was not party to the misdemeanour proceeding. Also, the holder of the information justified the refusal to satisfy the request for information with the circumstance that the misdemeanour proceeding material contains personal data and in pursuance of § 11 of the PDPA, the processing of personal data is only allowed with the consent of the data subject.

The special conditions, procedure and methods used for accessing procedure documents are set in the Code of Misdemeanour Procedure and it states that during the misdemeanour process, only the parties to the misdemeanour process my access the data gathered during the misdemeanour process, are in force until a decision has been made concerning the misdemeanour process or the regulation terminating the misdemeanour process enters effects and from that moment the PDPA applies in full effect to the access of the procedure documents.

The referral by the holder of the information to § 11 of the PDPA and to the personal data contained in the documentation concerning misdemeanour was appropriate, but not legitimate. Namely, the holder of the information is obliged to, pursuant to § 35 (1.11) of the PIA, to declare information internal, which contains personal data and if the disclosure of such data or allowing access to such data substantially violates the inviolability of life of the data subject.

Therefore, the holder of information has the right whether disclosing information that contains personal data violates substantially the inviolability of life of the data subject. But § 36 of the PIA, which states the criteria, which prohibit the holder of information in declaring information internal, limits this right. According to § 36 (1.12) of the Public Information Act, information is considered as such if it is for state or supervisory control or for disciplinary control and if the information is precepts or stated legal instruments and information concerning valid penalties.
Taking into account the aforementioned, § 35 (1.1 and 1.2) of the PIA and § 62 of the

14 SG I 2002.50.131; 110.654; 2003.26.156; 83.557; 88.590; 2004.46.329; 54.387; 54.390; 56.403; 2005.39.308; 40.311; SG III 2004.9.96

Code of Misdemeanour Procedure, the fine decisions made by the body conducting extra-judicial proceedings are considered as public knowledge, which should not be considered as internal information.

All of the aforementioned provisions practically forbid the disclosure of information during the misdemeanour proceeding, but not after the decision take effect. As the misdemeanour decision and the misdemeanour report contain personal data, which, if disclosed, could significantly damage the personal life of the data subject, like the subjects home address, identification code etc, § 38 (2) of the PIA provides access to the information or documentation, if access to the information could cause the disclosure of information with access limitations, to only that part of the information or documentation (recorded information or parts of documents), to which the access limitations do not apply.

The holder of information acted in concordance with the Public Information Act in dealing with the information request.

A lot of memorandums were sent to the Data Protection Inspectorate stating the failure of meeting the need for disclosure of public data. A significant number of holders of information have failed to disclose information that is to be disclosed on their Internet pages, also, they do not disclose topical information nor update their web page as often as necessary.

Such a situation is understandable, but not excusable, for smaller local governments, where only a handful of citizens have an Internet connection, but in addition to that, many state authorities have failed to update information or have updated it without regard to regulations.

One of the obligations of the Data Protection Inspectorate is also the clarification of the Public Information Act and legislation related to the Act and providing better access to information for holders of information and for providing better opportunities for creating advisory guidelines. The aforementioned activity is mainly visible from the number of clarification requests, which were answered on 36 occasions.

Overview of the activity of the DPI in workgroups of the European Union

The DPI is continuously working outside the borders of Estonia, mainly by participating in workgroups and projects:
The main workgroups are:
Article 29 of the Data Protection Working Party[15] - based on Article 29 of Directive 94/46/EC concerning the protection of the individual upon employment of the individual. The goal of the working party is to provide an expert opinion on data protection to the European Committee from the level member state level; to promote through cooperation between data protection authorities the application of the requirements of the Directive in member states; to council the Committee on human rights and freedoms that are related to data protection; to provide the general public with data protection recommendations.

The members of the Working Party are the representatives of data protection authorities from member states of the European Union. Representatives of data protection authorities from non-member states (Iceland, Switzerland, Norway) and representatives from potential member states (Bulgaria, Romania) also participate in the meetings. The working party meets 5 times per year. The main topics under discussion during 2005 were: biometric data and their usage in different walks of life; submitting flight passenger data to law enforcement authorities in USA, Canada, Australia, New-Zeland; geolocalisation data and their usage; preservation and providing access to traffic information (in the meaning of telecommunications); medicinal data; Binding Corporate Rules; e-mail services and data related to it etc.

Europol – On the 26th of January 2005, the Riigikogu accepted the act of joining of the European Police Board Convention (Europol Convention), based on Article K.3 of the Convention of the European Union) and it's protocols. Estonia will become a fully authorized member of the Convention after three months of the ratification of the joining act. The main goal of the European Police Board is to improve the effectively of competent authorities, with the provisions with the Europol Convention, and to improve cooperation for the prevention and fight against terrorism, illegal trafficking of narcotic substances or other forms of grave international crimes, which are related to organized crime and can be proven as such as it is known that two or more member states are involved in the case and, dependant on the extent, meaning and possible consequences, requires an international cooperative approach. For achieving the aforementioned goals, the main goals of Europol are to simplify communication between member states, to procure, compare and analyse information and secret documents, to immediately notify through the competent authorities set forth in Article 4 of the convention, the competent authorities of member states about information concerning them and of all crimes, to help the member states with their proceedings by continuously providing appropriate information to state departments and to maintain the computerized information system.

Therefore, by joining the convention, the Republic of Estonia took upon itself the obligation to participate in the work of Europol, to inform Europol on its own initiative of everything related to the fulfilment of the goals of Europol, to react appropriately to all requests for information by Europol concerning data, secret

15 http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/index_en.htm

materials and counsel, to keep information secret and to keep the secret information appropriate, to evaluate and submit information and secret information to competent authorities based on state legislation, to present Europol with requests of assistance concerning recommendations, information, secret information and analysis, to give Europol information concerning the storage of information in the computerized system, the ensure that the communication between Europol and itself is lawful and does not infringe upon any legislation.

By joining the convention, Estonia also took upon itself the obligation to achieve the previously mentioned goals and to follow the general provisions of the convention concerning information processing, including strict data usage provisions. The responsibility for information stored at Europol, for collecting information, submitting information to Europol and inserting information and the responsibility for the accuracy, timeliness and storage limitations of the information lies on the shoulders of the member state, which stored or submitted the information. Therefore, the transferral of information to Europol must be done by accurately following the provisions set in the convention.

By joining the convention, the Data Protection Inspectorate also received new obligations. Namely, the DPI was named as the state supervisory authority with the Europol Convention and its protocols and Article 23 of the Act, and the DPI must, based on local legislation, monitor the adding, accessing and transmitting of information to Europol and ensure that the rights of the data subject are not violated during this process. In addition to the aforementioned the Data Protection Inspectorate participates in the cooperative supervisory authority based on Article 24 of the Europol convention. The goal of the cooperative supervisory authority is to, in conjunction with the Europol convention, monitor the activities of Europol ensuring that data storage, processing and usage does not violate the rights of individuals. The competence of the cooperative supervisory authority covers reviewing the cases related to the processing and interpreting personal data, reviewing cases independently carried out by the competent authorities of member states, reviewing cases related to the right to receive information and finding solutions to any problems that should arise.

In addition to participating in the cooperative supervisory authority of Europol, the Data Protection Inspectorate also participates in the work of the Convention on customs information technology cooperative supervisory authority and as a reviewer of the work of the Schengen Convention cooperative supervisory authority.

In addition to participating in the work of workgroups, the DPI is also active in the INTERREG IIIC e-PRODAT project[16], which aims to develop the best solutions/experience for usable and creatable e-services, data protection standards based on the cooperation of supervisory authorities and other organizations and eventually release handbooks and instruction materials.

To achieve these goals, questionnaire has been compiled which will help to determine the problems with personal data protection and government electronic systems. The preliminary results of the questionnaire can be found on the web page of the project.

16 http://www.eprodat.org

Summary and findings

More and more people acknowledge their rights for inviolability of life and apply this right for accessing information meant for public use. This, in turn, raises the awareness of the processors of personal data and positively affects the performance of exercising the provisions set in legislation. The Inspectorate is continuously working for increasing the awareness of both citizens and data processors. If the data subject or the person making a request for information knows his or her rights and the holder of information or the process know their obligations, then the legality is ensured even without the intervention without Inspectorate. But due to the lack of human resources, notifying and training of the public and processors, also the amendment and equalization of legislation has not been provided in the desired extent. Therefore the Inspectorate is operating, at the moment, mainly as a supervisory authority and is only able to fulfil some of its pre-assigned obligations – providing the timely and correct servicing of the subject.[17]

One of the main directions of the Inspectorate for next year is training and increasing awareness in both DPI officials and processors. As Estonia is yet to join the major EU information systems (Schengen, Europol, Information security system of the Customs board, VIS, Eurodac) and as it cannot take place before the state systems have registered the processing of sensitive personal data with DPI, then the supervisory role of the Inspectorate will increase considerably. This, in turn, would mean that the officials of the Inspectorate must be trained in the respective legislation field. In addition to that, the awareness of the processors is constantly being improved though training in order to ensure the better application of processing regulations. In addition to training, covering the protection of personal data and the need for information disclosure in the media will increase the awareness. The DPI will put more emphasis on this.

In addition to that, the Data Protection Inspectorate will pay more attention to the fact that in order to participate more actively in the decision making process of the EU and to be able to use the received information more efficiently, the Ministry of Internal Affair must create an official position which deals with the development and implementation of data protection policies. The domain of data protection concerns all areas of government an in order, both on the level of the state and the level of the EU, to participate in negotiations as equal partners, the position of the data protection representative must be present within the structure of the ministry.

17 Overview of the activities of the Data Protection Inspectorate, 2005, first half year

Statistics

Name	*2003*	*2004*	*2005*	*Remarks*
Presented registration applications	497	390	368	
Registered	289	314	361	
Registration refused	170	76	29	
Control	49	35	28	
Inc. follow-up control	16	8	8	
Inc. pre-assigned control	3	8	3	
Precept to the processor	37	28	4	
Notice of processing of private personal data	0	6	0	
Opinions concerning state record instruments of constitution	27	40	16	
Procedure				
Challenges (PIA)	49	34	40	
Precepts (PIA)	13	7	9	
Complaints and memorandums (PDPA)	98	27	41	2003. elections
Misdemeanour procedures	14	5	5	
Enforcement orders	4	6	4	
Other				
Opinions concerning drafts	57	50	48	
Trainings	21	15	30	