DATA PROTECTION INSPECTORATE

REPORT CONCERNING THE PERFORMANCE OF THE PERSONAL DATA PROTECTION ACT AND THE PUBLIC INFORMATION ACT

2006

CONTENTS

Honourable Riigikogu Constitutional Committee members and Chancellor of Justice,

On 19 July, ten years passed since requirements were enforced by law for the processing of personal data in the Republic of Estonia. Gradually, the parties involved in the processing of personal data have, on the one hand, started to regard their obligations more seriously while, on the other hand, they have become more aware of their rights.

Pursuant to the character of supervisory agencies, our obligation is to observe and assist people in understanding and becoming aware of their rights regarding the inviolability of private life and to place distributed information into general use.

Development indicators are the large number of reports, memoranda, inquiries, complaints and challenges we receive. This, in turn, proves that awareness of the field is no longer the knowledge of a limited number of people.

Certainly, everything has not gone swimmingly, so far. It is still not entirely understood that the Data Protection Inspectorate helps to create trustworthiness in terms of the state, being an independent institution, ensuring balance, on the one hand, for information requested by personal data processors and, on the other hand, the wishes of the data subjects that the processing would take place in conjunction with the law.

In order to ensure continuity, we are continuing to work actively with persons and processors in the raising of the awareness of the law. If people are aware of their rights and the holder of information or personal data processors their obligations, then the rights of the person are guaranteed without direct interference by the supervisory agency.

I consider another significant indicator to be the significant expansion of the agencies supervisory activities. I hope that after a while the Data Protection Inspectorate will have changed from a registrar to a surveillance agency.

I would like to thank, sincerely and from the heart, everyone whom I came into contact with during the course of my everyday work, for their pleasant co-operation.

I encourage people to use their rights more often and present questions to both themselves as well employees and the holders of information.

Sincerely,

Urmas Kukk
Director General Data Protection Inspectorate

Regarding the Inspectorate

The right of persons to protect their private life, secrecy of information exchange and data protection, is prescribed by the Constitution of the Republic of Estonia[1]. According to the constitution, state agencies, local governments and their officials are not allowed to gather or record data against the will of a citizen of Estonia, about their beliefs; everyone has the right to the secrecy of messages they communicate or that are communicated to them via mail, telegraph, telephone or other generally used means. The inviolability of a person's private life can only be limited by the permission of the court to prevent criminal activity or for the gathering of evidence during a criminal proceeding, according to the methods and cases provided by law.

Pursuant to the constitution, state agencies, local governments and their officials have an obligation to provide citizens, at their request, with information about the activities of the agency, except for information, the publication of which is prohibited by law and information which is intended, without exception, for internal use. According to the procedure prescribed by law, Estonian citizens have the right to familiarize themselves with information about themselves held by state agencies and local governments, as well as stored in their agencies archives.

The Data Protection Inspectorate (hereinafter: AKI) is a state supervisory agency operating under the administrative area of the Ministry of Internal Affairs, whose primary objective is the protection of persons constitutional rights and freedoms in the processing of personal data and ensuring a persons right to receive, for free, information distributed for public use.

Pursuant to these objectives, the primary tasks of AKI are the performance of independent supervision of the legality of the processing of personal data and the maintenance of databases on the one part and the performance of information requests on the other part.

In addition to the above mentioned the Inspectorate registers the processing of sensitive personal data, performs supervision of database maintenance and applies, within the limits of its jurisdiction (including Personal Data Protection Act[2] or Public Information Act[3]), administrative coercion or criminal proceedings in the event of a violation of obligations arising from

[1] Eesti Vabariigi Põhiseadus. RT 1992, 26, 349; 2003, 29, 174; 64, 429
[2] Isikuandmete kaitse seadus. RT I 2003, 26, 158; 2004, 30, 208
[3] Avaliku teabe seadus. RT I 2000, 92.597; 2002, 61,375; 63, 387; 2003, 25, 153; 26, 158; 2004, 81,542; 2005, 39, 308

legislation. Together with the Communications Board, the inspectorate also performs supervision regarding compliance with the requirements of the Information Society Services Act.

This report is sixth pursuant to the monitoring procedure of the Public Information Act (hereinafter: AvTS) and fourth pursuant to the monitoring procedure of the Personal Data Protection Act (hereinafter IKS). The report provides an overview of the more significant events and facts that took place in 2006 in the fields of public information and personal data protection.

The amount of resources allocated for the inspectorates 2006 budget is EEK 7 922 473. The composition of employees in the inspectorate as of 31 October 2006 was 23 officials, with 21.5 posts filled (three officials hold office on a part-time basis).

The supervisory agency is divided into three units: control unit, development and analysis unit and the general unit. The control unit is made up of the registration, procedure and inspection services. There are 31 offices in the AKI structure, of which 9.5 offices are unfilled.

On 11 November 2006, changes in the statutes of the Data Protection Inspectorate entered into force. The primary novations are the prescription of the jurisdiction of the director general's deputy and the specification of the obligations of monitoring in terms of the processing of personal data arising from European Union legislation.

Surveillance of the processing of personal data

Raising the awareness of persons

In the current accounting period a significant portion of AKI’s activity was directed towards citizens and raising awareness about data processing, with the goal of informing citizens and personal data processors about their rights and obligations. The correctness of the development direction begun is testified to by the increase in the number of questions, requests for explanation and requests for information submitted in writing and by telephone. In addition to the above mentioned the inspectorate has actively participated in various information days and training seminars.

In the current year, local governments and educational institutions (both students and teachers) have come under scrutiny. In the case of the latter, the need for training has raised problems and, to a great extent, questions related to personal data processed by educational institutions and student evaluations being performed. For the possible resolution/prevention of shortcomings and for the better application of educational institutions corresponding work the Ministry of

Education and Research is preparing a student evaluation methodology, and the inspectorate has made its own suggestions.

In addition to the above mentioned fields, a training day was held for pharmacists, Pension Board employees, Border Guard officials, vital statistics office employees, population register employees, librarians, E-health Foundation, Private Forest Centre, local government IT directors, etc. There were a total of 34 training seminars, in which 1300 persons participated.

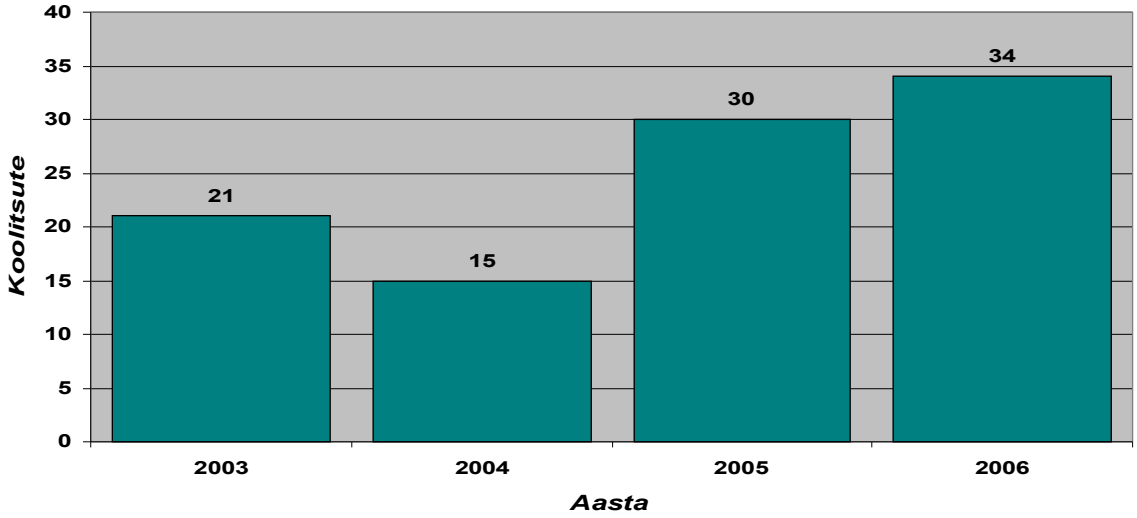

Figure 1. Training seminars carried out by Inspectorate officials, by years

AKI officials participated in the computer training seminars, administrative proceeding, misdemeanour procedure and language in-service training. In the following period, continuing training is planned in the mentioned fields.

Registration of processing

During the period 01 October 2005 to 30 September 2006, the Data Protection Inspectorate received 414 registration applications, of which 103 were first time and 241 repeat (see Figure 2:

During the given period, 229 registration applications were approved (see Figure 2). The registration for the processing of sensitive personal data was refused in two cases and two applications were left unreviewed. The difference in the number of applications received and the number of registration decisions is a result of the fact that an application is accepted into proceeding during the reference period, but the registration has already taken place outside of the reporting period.

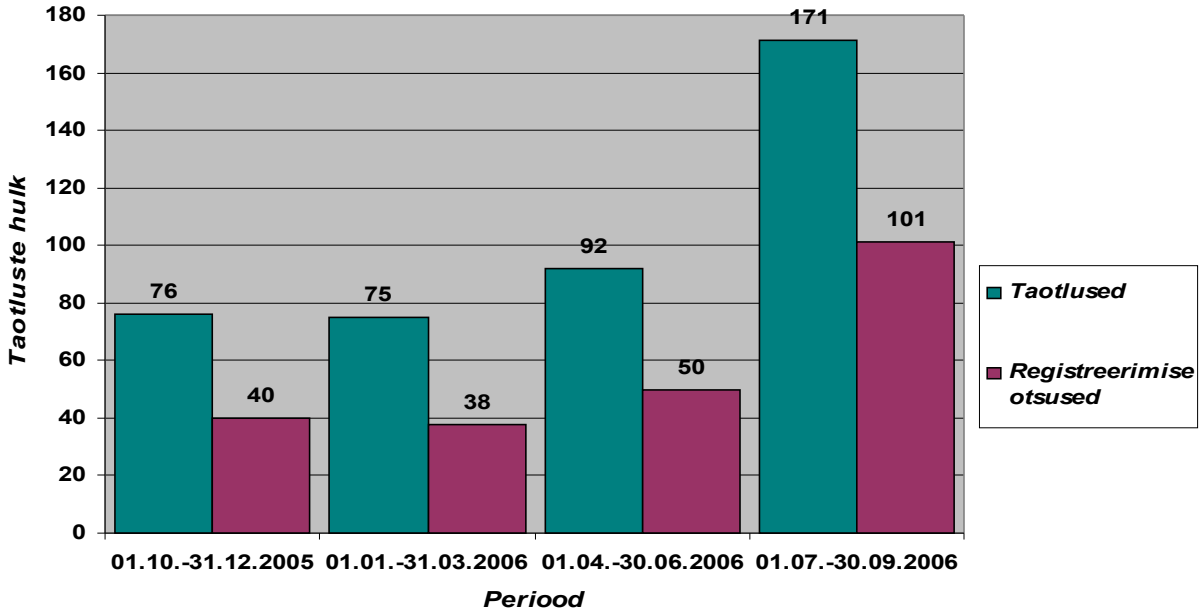

Figure 2. Number of received applications and the number or registered sensitive information processed

On October 1 of the current year, the registration deadline for a large number of sensitive information processors ended. The deadline originated with the entry into force in 2003 of the implementing provisions of the Personal Data Protection Act. Decisions regarding the registration of sensitive information processing that were issued before the previously named date were valid for 3 years, as of 1 October 2003. Registration applications for sensitive information processing regarding those not yet submitted (sensitive personal data processing registration deadline has passed for ca 600 employees) are marked for implementation of administrative coercion. This ensures the equal treatment of employees who have registered on time for sensitive information processing.

The inspectorate prepared, during the period 1 October 2005 to 30 September 2006, 4 precepts for data workers, 3 warnings and in once case a penalty payment of EEK 8000 (Health Care Board) was implemented, and in another instance a penalty payment in the amount of EEK 10 000 (Tartu University Hospital).

The primary shortcoming for employees in the implementation of personal data processing requirements is the passive performance of the registration obligation. The pharmacy service providers can be cited as an example, for which, during the reporting period, only 3 service providers registered for sensitive information processing.

There are an estimated 300 companies providing this type of service in Estonia, for whom penalty payments will be applied in the following accounting period for not performing the required registration obligation.

The Data Protection Inspectorate participated in the information day arranged by the State Agency of Medicines and held a personal data processing requirements training seminar for the target group.

A similar operating model is indigenous to local county governments and local governments, in the case of which the inspectorate has prepared similar activities for guaranteeing the performance of obligations pursuant to law.

In addition to the registration requirement for the processing of sensitive personal data the inspectorate is including the requirement for corresponding workers to register changes implemented in the processing of personal data.

Both obligations must be fulfilled either before beginning personal data processing or the implementation of changes and the objective is to ensure the legitimate processing of sensitive personal data.

It must be admitted that the responsible employees have become more active in the last accounting period in the performance of the required obligations.

Not registering on time for the processing obligation may bring with it a situation where the responsible employee has created a software based solution for the processing of sensitive personal data (register, information system, etc.), placed it into use, and in certain cases allowed third party persons to use it.

Based on the above described, the first information regarding these types of solutions arrived at the Inspectorate during the course of surveillance and it may appear that the implemented methods are not in concert with the Personal Data Protection Act.

In addition to the fact that it involves the violation of personal data processing requirements, the situation also includes the risk of large monetary damage to responsible employees. The present operating system must be brought into compliance with requirements arising from legislation which, as a rule, is typically more resource intensive, than if the implementation of changes were to have taken place in the systems design stage.

The next largest shortcoming in the field of registration is not implementing security methods. The primary reason for leaving methods unimplemented is that in the estimation of data processors the implementation of methods is too costly (for example, smaller regional health care providers do not want to purchase the required paper shredder) or have not planned for this type of expenditure in their budget (for example, the school does not purchase security cabinets for nurses' ambulatory carts).

The situation in which security methods, which aren't actually implemented, are described so that the registration decision is received can also be described as inappropriate.

A significant omission is not performing the obligation of notifying the data subjects. For example, in the medical sector each health care service provider must have developed and made available to data subjects a client service standard[4], which must contain at least the following:

1) method for the registration of complaints, their resolution and providing of feedback to patients;

2) patient's rights and obligations;

3) communication with the patient and their family;

4) process for the informing of patients regarding the provision of health care service;

5) the on time notification of patients in registering for the waiting list, their direction between health care service providers and in the substitution of health care professionals.

Requests for explanations received by the Inspectorate's registration division concern, for the most part, what is related to the registration applications preparation and submission, the submission of various categories of personal data, permissibility of the processing personal data and consent relating to form and content. In regards to frequently asked questions, AKI has published its clarifications on its website.

A suitable specific example for expressing the more frequently occurring problems is the case of the processing of sensitive personal data in the framework of a single investigation. The investigation was ordered by the Statistical Office, which used the authorised processor Tallinn University Institute of Estonian Demography.

The investigation was carried out without the holding of an authorisation for sensitive personal data processing and the Data Protection Inspectorate received information through the mediation

[4] RTL, 28.12.2004, 158, 2376

of citizens' complaints. Nearly 8000 persons were included in the investigation, and included in the data collected was information about their state of health, sexual life, etc.

Regardless of the willingness by the data subjects to participate in the investigation, the informing of the data subjects pursuant to § 12 (2) of the Personal Data Protection Act did not take place pursuant to prescribed conditions. The requirement for informed consent is the primary safeguard for the rights of a data subject and the objective is to allow the data subject to be provided with information from all perspectives for the making of a decision regarding consent, including evaluating the accompanying risks and possible consequences, or in a simplified definition – to understand, who, why and how their data is come into contact with.

The obligation to inform rests with responsible and authorised processors and involves a so-called active responsibility. In order that the data subject would be able to make a decision about allowing the processing of their data, it is necessary for them to be provided with information from all perspectives regarding what the decision brings along with it.

The obligations of authorised processors regarding the preservation of personal data and its transfer to responsible data processors is not clearly designated, as a result of which they are also currently in the situation where contractual relationships have ended or have been terminated between parties, in the domain of authorised processors, and the latter disregards the offers made by responsible data processors for the transfer of the data to the State Archives. At the same time, the responsible processor has not presented specific requirements and has not used the opportunities at its disposal to bring an end to the illegal situation.

The Statistical Office's activities in relations with the Inspectorate have been contradictory. Among other things, it has been claimed that there has never been a contractual relationship between the responsible processor and authorised processors, the data to be preserved does not allow for the identification of persons, etc.

Regardless of the question concerning the identification of persons, the position has been taken that the state of the collected data does not allow for the identification of the data subject and that for demagogic reasons an attempt has been made to disregard the evaluation of the risk of indirect identification. The collected questionnaires, together with the interview reports, contain the data subjects' given name, home address, telephone number, information regarding the data subjects' education and career, last job, etc.

The composition of the named data allows for the identification of the data subjects through the use of public sources of information. It is because of this that it doesn't matter what group of people the data is being collected about. According to the Statistical Offices assessment, it is not possible to identify persons based on the composition of the given data.

By taking this position, it allows all those who wish to do so to access to the collected data, since it is as if the limits prescribed by law, which should protect the data subject, are not applicable.

The evaluation of the risk of the direct or indirect identification of the person is of determinative importance in the processing of data and a careless attitude regarding this question may bring with it a very large scale grazing of the inviolability of the data subject's private life together with material and moral damage.

Handling data reflecting the private sphere of a person's life with the above described carelessness, disregarding obligations arising from the law and thereby also the rights of the data subject to information, is expressed in a particularly cynical and careless attitude towards the data subjects' rights as a whole.

Complaint proceedings

During the accounting period, 110 complaints, clarifications and memoranda were received by the Data Protection Inspectorate (see also Figure 3), 10 misdemeanour proceedings were begun, 11 misdemeanour decisions were made (on the basis of IKS).

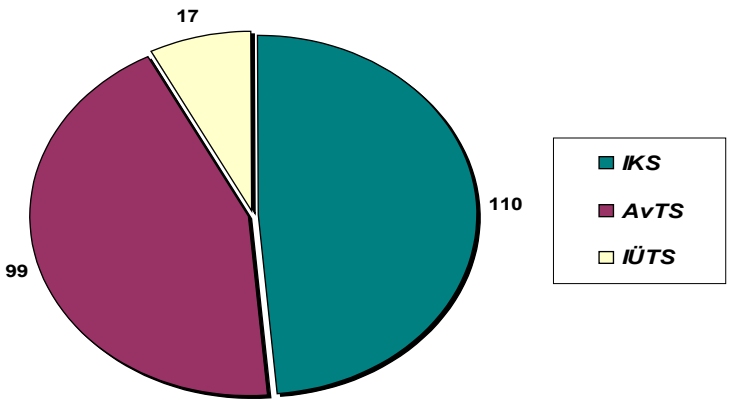

Figure 3. Complaints, challenges, memoranda and requests for explanation received during the period 01 October 2005 – 30 September 2006, by law

The running theme for both requests for complaints as well as requests for explanation have been credit information related problems, where persons complain or ask for an explanation if and under what basis their personal data has been published on the Estonian Credit Register homepage and is available to the public.

Cases

Publication of payment arrears

Questions are raised regarding the www.economy.ee homepage, primarily on the topic of: who, what and on what basis is data published. Included in the debates over these topics, this year, are the Chancellor of Justice, banks as well as communications operators.

The primary set of problems concerns the availability of personal data on the Internet - personal data (personal identification codes, address, etc.) is published on various forums and homepages

Julianuse Inkasso Agentuur AS published the names of persons in their debtors list. The Data Protection Inspectorate made a misdemeanour judgment, with which Julianuse Inkasso Agentuur AS was assessed a monetary fine for the unlawful publication of data.

Persons sick leave certificates - medical treatment invoices on the highway

On 3 August 2005, a notice was communicated from the newspaper “Sillamäe Vestnik“ that on 30 July 2005 a passer-by found, on the highway near the city of Sillamäe, the 1998 D-part of the sick leave certificates for those that had visited the Narva Haigla women’s consultancy.

During the proceeding it became clear that the 248 found certificate for sick leave D-parts are sick leave certificate-medical treatment invoices, which were made up of parts A,B,C,D and were in use from 1996 to 1999.

The A and B parts were issued, in part, centrally and given to patients, the C part was forwarded to the health insurance fund and the D-part was returned to the person who issued the certificate for sick leave. The D-part was preserved for 3 years and destroyed together with the certificate for sick leave registration book, whose preservation period was also 3 years. In the given case, the D-parts of the certificate for sick leave should have been destroyed in 2001, which, however, was not done.

The destruction of documents containing sensitive personal data in the SA Narva Haigla took place before 2002 by burning, for which according to available testimony a corresponding

contract was concluded with the boiler plant operating in the Narva treatment system, at the time of the proceedings it is no longer possible to control the existence of the contract.

When and by who the found D-parts were actually taken for destruction is not possible to determine, since the destruction certificates for the documents were absent. SA Narva Haigla also failed to control whether the documents containing sensitive personal information, which were sent for destruction, were actually destroyed or not. As a result of this a situation occurred where certificates for sick leave containing sensitive personal data became available to everyone.

SA Narva Haigla offers residents consultation services with general practitioners and medical specialists, during the course of which personal data describing the patients' state of health are processed. According to the Personal Data Protection Act § 4 (3) 3) a person's data describing their state of health is sensitive and Personal Data Protection Act § 6 (6) must be followed during its processing, pursuant to which the responsible and authorised processor of the data is required to follow the security principles during the processing of personal data. According to the security principles, to protect personal data security measures must be implemented to prevent their unwanted or unauthorised amendment, their publication or to prevent their destruction.

During the misdemeanour proceeding it was discovered that SA Narva Haigla did not implement for the protection of personal data, the required organisational, physical and information technology security methods as prescribed by IKS § 6 and § 19.

Pursuant to this, on 6 June 2006 AKI prepared an expedited procedure decision, pursuant to which SA Narva Haigla was issued a monetary fine in the amount of EEK 15 000.

Issuing of data from the register of persons liable to service in the Defence Forces

AKI began a misdemeanour proceeding regarding the matter where Mindworks Industries OÜ had concluded an agreement with the Northern Department of National Defence for development work regarding the register of persons liable to service in the Defence Forces and for its applications. As a result of this, the private limited company changed, pursuant to § 8 of the Personal Data Protection Act, into an authorised processor of personal data.

In June of 2005, one of the employees of the authorised processor took with him from the then Northern Department of National Defence, upon completion of his duties, a USB memory stick on which was saved, in unencrypted form, data for 302 067 men.

It involved male citizens born between the years 1950 and 1987, or in other words the data of all persons liable for service in the Republic of Estonia military. The data contained personal identification codes, given and surnames, father's names and place of residence. The employee lost the above named memory stick, along with the data saved on it, in Tammsaare Park in Tallinn, near the Estonia theatre.

The described loss was made possible because Mindworks Industries OÜ did not implement the required organisational, physical or information technology security measures prescribed by the Personal Data Protection Act for the processing of personal data.

This resulted in the violation of IKS § 19 (1) 3), pursuant to which the responsible and authorised processor is required to place into use organisational, physical and information technology security measures regarding the protection of the confidentiality of personal data from unauthorised processing.

Pursuant to subsection 2, clause 6 of the same section the authorised processor is required to ensure that with the forwarding of personal data via data communication equipment and transporting via data mediums, the arbitrary reading, copying, amending or deletion does not take place.

Pursuant to IKS § 19 (2) 7), the responsible and authorised processor is required to design the organisation of work in the company, agency or association in such a manner as to allow for the performance of data protection requirements.

IKS § 20 (3) requires the responsible and authorised processor to ensure the training of persons working as subordinates in personal data processing.

In May of 2006, AKI prepared a proceeding-decision, with which a monetary find in the amount of EEK 15 000 was assessed to Mindworks Industries OÜ for the violation of IKS § 19 (1) 3), IKS § 19 (2) 6) and 7) as well as IKS § 20 (3).

Performance of surveillance

During the accounting period, AKI inspection service performed 48 on-site verification visits for the performance of the Personal Data Protection Act.

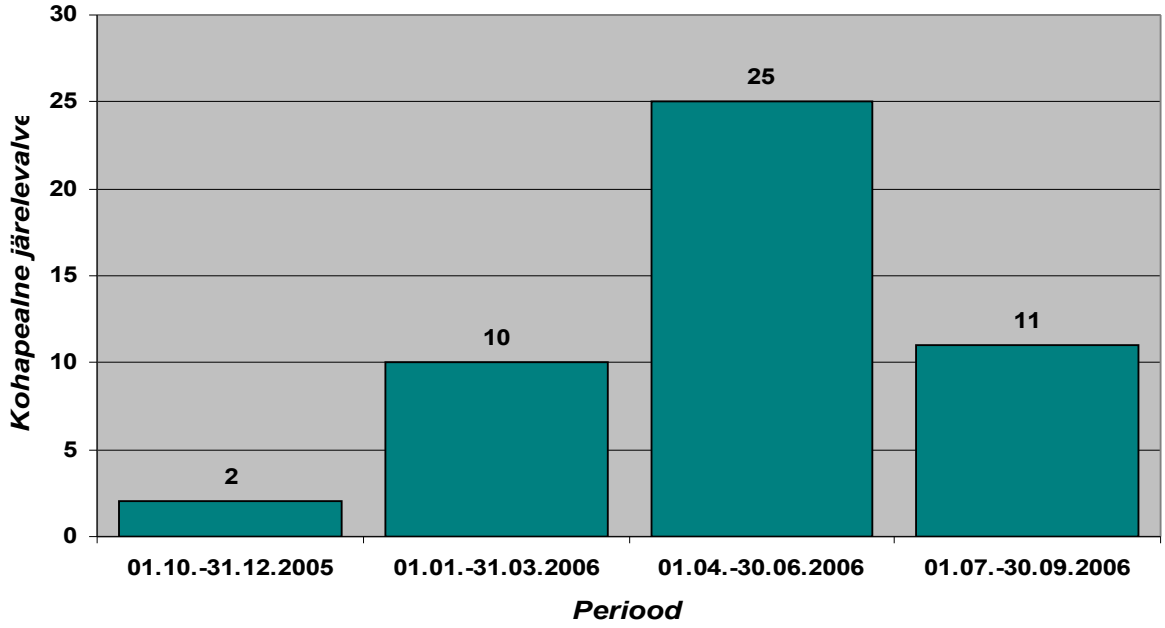

Figure 4. Number of performed on-site inspections by period

Viewing figure 4, it can be seen that during the accounting period the number of verification visits varied. In the third time period presented, the observable number of verification visits showed a marked increase. The reason behind this was that in the period 01 October -31 December 2005, there was only 1 official employed at the inspection service.

Cases

In several instances, data processors have been hindered in their performance of data protection requirements because larger foreign software manufacturers consider Estonia to be small and do not offer a sufficient quality support service. In addition, a problem has occurred in the ordering of software, where the volume of orders by Estonian clients has been somewhat small and because of this the software manufacturers are not interested in negotiating the terms and conditions of contracts.

Eurodac proceeding

Eurodac is the 11 December 2000 regulation No 2725/2000[5] of the Council of the European Union, which treats the establishment of the Eurodac system for the comparison of fingerprints with the objective being the effective application of the Dublin convention, a fingerprint comparison system for a specific group of asylum applicants and illegal immigrants, which is in use in all European Union member states (except for Denmark) and third countries (Norway and

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000R2725:EN:HTML

Iceland) connected to the Eurodac order. In the Eurodac system, each participating state takes the fingerprints of all asylum applicants over the age of 14. The taken fingerprints are compared with other data entered into the database. If the system shows that the fingerprints have already been saved, the asylum applicant is sent back to the state where their fingerprints were first registered.

Access to the system is granted only on the basis of the objectives contained in the Eurodac regulation. The names or other personal data of persons are not kept in the database; instead it is solely based upon a biometric comparison, which is a more secure and accessible method of identification. The Eurodac system is comprised of a central processing unit located at the commission, where there is a fully automated computerised central database for the comparison of the fingerprints of asylum applicants and the electronic data communication system of states and central units participating in the system. In Estonia, the only agency that has access to data saved in the central database of the Eurodac system, based upon Council regulation (EU) No 2725/2000 article 15 (1), is the Citizenship and Migration Board (hereinafter KMA).

Pursuant to Council of the European Union regulation No 2725/2000 article 19, the domestic supervisory agency in Estonia is the Data Protection Inspectorate. The task of the Data Protection Inspectorate is, following independent and concerned domestic legal provisions, to monitor the legality of data processing pursuant to the above mentioned regulation, including the communication of data to the central unit. Monitoring of the Eurodac central unit to ensure that the processing and use of the data stored in the central unit does not violate the rights of the data subject, belongs to the independent supervisory agency – the competency of the European Data Protection Supervisor created pursuant to article 286 (2) of the European Union memorandum of association. In addition to the above mentioned, the European Data Protection Supervisor also makes sure that the communication of personal data from the central unit to member states takes place pursuant to law.

In September 2005, a co-operation meeting between representatives of domestic data protection supervisory agencies and the European Data Protection Supervisor (EDPS) took place in Brussels. The primary theme of the meeting was the performance of monitoring of the Eurodac system It was agreed that three primary aspects, for which domestic supervisory agencies in the performance of supervision should, among other things, draw their attention to. These were “special searches” or category 9 inquiries (pursuant to Council of the European Union regulation No 2725/2000 article 18 (2) petitions from data subjects for obtaining information regarding

themselves contained in the Eurodac system), use of the Eurodac system for other purposes than the framework of the implementation of exile policies and the quality of communicated information. For the achievement of the implied objective, the number of category 9 inquiries communicated to the central unit by the competent authorities of member states was distributed (in the case of Estonia it was 10 inquiries).

In February of 2006, AKI communicated to KMA a request letter in which it gave notice of the beginning of the final state supervisory proceeding and requested data. On several occasions KMA has sent various Eurodac subject category data to the Eurodac central unit.

According to KMAs response, as of Estonia's joining the Eurodac system, communicated to the Eurodac central unit were 16 category 1 inquiries, of which in two instances the data was mistakenly communicated twice, and therefore the total number of inquiries was 14. There were no category 9 inquiries made during the previously mentioned period.

In March of 2006, AKI sent a request letter to the Ministry of Internal Affairs, in which a request was made for a list of national agencies which had access to the data saved in the Eurodac central database. A copy of the list of the above mentioned agencies was also requested, which the member state, pursuant to the Council of the European Union regulation No 2725/2000, had to communicate to the Commission of the European Communities.

According to the reply by the Ministry of Internal Affairs, KMA is and has been Estonia's only authorised agency, since joining the Eurodac system, that has access to the data saved in Eurodac's central database, and the only work station in Estonia connected to the Eurodac system is located in the KMA.

AKI officials carried out an on-site inspection of the KMA refugee division with the objective of inspecting the organisational, physical and information technology security methods, with which the implementation of the prescribed requirements of the Council of the European Union regulation No 2725/2000 article 14 are ensured. As well as an inspection of the legality of the inquiries communicated to the Eurodac central unit by KMA.

During the inspection process it became clear that there were deficiencies in the organisational and information technology security methods - one username and password were used by all employees to log into the work station and the FIT/NAP system supplied by Steria AS did not allow for extracts to be made from all data processing actions, and it was not possible to print out the logs for the inquiries made to the Eurodac central unit. Thus, during the course of the

supervisory operations the violation of the requirement prescribed by the Council of the European Union regulation No 2725/2000 article 14 (c) was established – to ensure that it is possible to control and afterwards make sure what type of data is saved in the Eurodac system, when and by whom it was done (data recording control).

In April of 2006 KMA sent to AKI all of the logs, received from the Eurodac central unit, for all data processing actions performed by KMA. From the list of logs it can be seen that the Eurodac central unit has been forwarded data on a total of 32 occasions, including 10 category 9 inquiries.

After which AKI communicated to KMA a request letter, in which it asked for clarification regarding the reasons which caused the discrepancy between the number of inquiries in KMAs response and all of those visible in the list of data processing action logs. A clarification was also requested for each entry: who, whose data and what for purpose they were forwarded to the Eurodac central unit.

In the response sent to AKI in May of 2006, it can be seen that inquiries regarding the Eurodac regulation (Council of the European Union regulation No 2725/2000 and No 407/2002[6]) were sent to the central unit on 17 occasions, of which the data was mistakenly sent twice on two occasions. Hence, the total number of legitimate inquiries sent to the central unit was 15 category 1 inquiries.

During the proceeding it was discovered that the remaining 17 inquiries were performed for testing the technical solution and demonstrating the system as being operational. The processor claims that the Eurodac system was presented to Ministry of Internal Affairs employees, other Baltic State colleagues as well as their own departments' employees. Inquiries were performed using KMA information gathered by KMAs own workers especially for testing (fingerprints, personal data - which was gathered in such a way that the data subjects were aware of what the data was to be used for). At the moment of the performance of the inquiries the performers of the inquiry were convinced that the given inquiries were performed correctly, therefore their actions lacked intent to violate requirements.

Pursuant to Council of the European Union regulation No 2725/2000 article 1, the only objective of the Eurodac system is to aid in determining which member state, according to the Dublin convention, is required to review the asylum application submitted in the member state, and facilitate the application of the Dublin convention. Hence, the use of Euordac system has been,

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002R0407:EN:HTML

on 17 occasions, non-intended, since the objective of the system does not foresee testing and presentations.

If some of the deficiencies in the organisational and information technology security methods were removed during the proceeding - logging into the workstation now takes place via ID cards – then it is still not possible for KMA at the current time, despite numerous attempts, to send logs to the Eurodac central unit.

According to the explanations given by KMA, they repeatedly turned towards the supplier of the of the software to the Republic of Estonia, necessary for the Eurodac system, Norwegian company STERIA AS, for a solution to the problem as well as concluding a new maintenance and support contract, but there was no response to their many requests.

During the course of the supervision proceedings it became clear that the Norwegian company STERIA AS, which supplied the necessary software to the Republic of Estonia for the Eurodac system, had concluded a "Licence Purchase Agreement" in 2004 with the Republic of Estonia Ministry of Internal Affairs, not KMA.

According to explanations given by the Ministry of Internal Affairs, in July of 2004, the STERIA AS representative stated during the course of the software demonstration that the logs for inquiries sent to Eurodac are saved and can be viewed. After this, the most frequent circumstance was not controlled and the lack of log-in access was not discovered before AKI employees requested their issuing in March of 2006.

On 31 August 2006, AKI prepared a precept for KMA to take the Eurodac system into compliance with Council of the European Union regulation No 2725/2000 article 14 (1) c) no later than 1 January 2007 and to present an overview to the Data Protection Inspectorate on 1 November 2006 regarding the work performed for fulfilling the precept and the executed operations.

In October of 2006, KMA sent a letter to AKI, in which it gave notice that KMA installed a software update in the Eurodac workstation, which allows for inspection and making sure afterwards which types of data are saved in the Eurodac system and at what time. The software update was received in August 2006, on the basis of the maintenance contract concluded between KMA and STERIA AS.

In order to inspect the information contained in the letter sent by KMA, in November 2006 AKI performed a third on-site inspection of the refugee section of KMA, during the course of which the following conditions were made clear:

1) In September of 2006, a new version of the NAP server software was installed, which allows for the viewing of the logs regarding inquiries made from Estonia to the Eurodac system as well as the data entered into the Eurodac system by Estonia;

2) According to the explanations given by KMA officials, the new version of the NAP server worked until November 2006, and a printout of the logs during that period has been made;

3) From the beginning of September 2006 until the end of November it was no longer possible, due to technical reasons, to enter the NAP server where the application for viewing logs is located;

4) According to KMA officials, the KMA information technology department has been notified of the technical problems associated with the NAP server, and they have repeatedly contacted STERIA AS to find a solution to the technical problems, however, at the current moment a solution to the problems has not been found.

KMA promised to notify AKI when a solution has been found for the NAP server's technical problems.

Surveillance of the performance of the Public Information Act

During the period of 1 October 2005 to 30 September 2006 the Data Protection Inspectorate received 99 requests for explanation, memoranda or challenges on the basis of the Public Information Act (AvTS) (see Figure 5) and on the basis of the submitted 8 misdemeanour proceedings were begun.

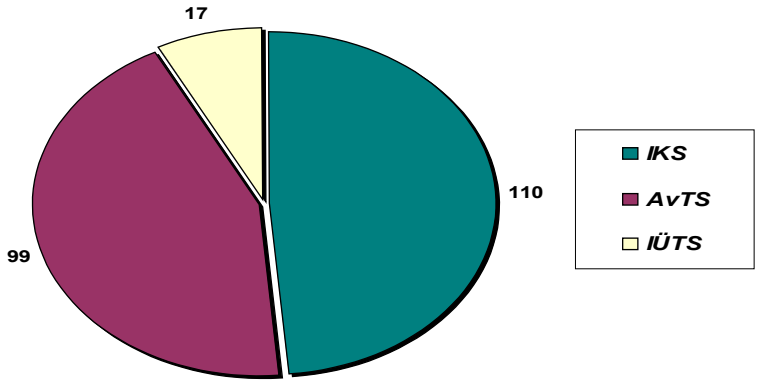

Figure 5. The complaints, challenges, memoranda, and requests for explanation in terms of laws during the period 01 October 2005 - 30 September 2006.

OF the challenges received by the Inspectorate, the majority were submitted in regards to violations of requirements for maintaining a website (state agencies, rural municipality governments) or based on the failure by the holder of information to comply with requests for information.

The majority of the violations regarding maintaining a website were in regards to an insufficient document registry or lack of a registry. Complaints were presented for documentation concerning misdemeanours and the publication of materials gathered during criminal proceedings after the conclusion of the corresponding proceedings.

Situations have become evident where documents are declared for internal use, for which the designation of a restriction on access was illegal. An example of these cases are the directives of the Ministry of Social Affairs regarding additional remuneration, where the legitimate situation was restored during the course of the proceedings, and the incident with the Committee on Decorations, as a result of the proceeding a precept was prepared.

The theme running throughout the submitted memoranda was the violation of the maintenance of the document register and website requirements.

With the goal of harmonising the performance of administrative training by AvTS, AKI issued a uniform position on the publication of personal data in local government regulations and orders.

Based on the fact that at the present time rapidly developing information technology allows for the creation of a legitimately published database of personal data, the objective for the use of which can no longer be controlled later, and therefore the inviolability of the data subjects private lives is not guaranteed, AKI is of the position that the requirement for the publication of legislation does not mean the unlimited publication of personal data nor access to personal data via a website.

As a result, websites should contain disclosed information regarding how the financial resources of a state are used and for the disclosure of personal data they should, above all else, abide by the principle of minimalism and the inviolability of private life.

Cases

Ministry of Defence

The Data Protection Inspectorate received a notice from the Ministry of Defence regarding the violation of the Public Information Act. In the notice, the initiation of a misdemeanour proceeding was requested for the prosecution of the preparer of the documents, for not marking the documents for internal use only. According to the notice, the Tapa Training Centre had not enforced in its letter the restriction on access to documents containing information, which contains personal data pursuant to AvTS § 35 (1) 10) and the documents were left unmarked.

AKI did not begin a misdemeanour proceeding on the basis of the notification of a misdemeanour in the letter dated 23 August 2006, in connection with the leaving of an internal use document unmarked, since according to AvTS § 54^1 (1) the knowing release of incorrect public information

or knowing disclosure or release of information intended for internal use or leaving the precepts issued by the Data Protection Inspectorate unperformed is a punishable offence.

Pursuant to AvTS § 34 (2) the head of an agency may establish a restriction on access to information and classify information as information intended for internal use Pursuant to AvTS § 35 (1) an exhaustive list of the grounds on which the holder of information is required to classify information for internal use. If allowing access to information may result in the disclosure of restricted information, then access is ensured only to the part of the information or document to which restrictions on access do not apply may be accessed (AvTS 38 (2).

Pursuant to the Public Information Act, a punishable offence in a misdemeanour proceeding is the knowing release of incorrect public information or knowing disclosure or release of information intended for internal use or leaving the precepts issued by AKI unperformed. AvTS does not foresee misdemeanour liability for the holder of information upon the initial discovery of the failure to establish restrictions on access to information provided by law. If the holder of information violates the restrictions established by law for access to the information, AKI has the right to at first issue a precept to the holder of information in order to restore the legal situation. The right to apply sanctions only arises here from the failure to perform the precepts issued by the inspectorate. Misdemeanour responsibility is only stipulated in the instance where information prescribed for internal use is released or disclosed.

The portion of the letter from the Tapa Central Training Centre containing personal data has been designated for internal use with letter No TV2.14/3954-2.
Since the portion of the abovementioned document containing personal data has a restriction on access enforced and the legitimate situation was restored, the inspectorate lacked a basis for issuing a precept.

In case an official has not performed obligations assigned to him, i.e. enforcing the restriction on access to documents on time, this incident must be heard in a supervisory control proceeding.

Since no names were disclosed in the 27 July 2006 article “Suur allahindlus Kaitseväes” published by Eesti Ekspress, as a result of which the public disclosure of private life or sensitive personal data or the violation of the inviolability of private life, then it was left unexplained what the misdemeanour notice was based upon, that the personal data of persons eligible to be drafted was disclosed.

AKI found that it was not plausible or expedient on the part of the inspectorate to perform state oversight based on the operations procedure, over the following of prescribed requirements. The resolution of these types of violations belongs to the jurisdiction or supervisory control of a superior body or agency, as a result of which the regulator has designated supervision over compliance with this act in AvTS § 44.

Based upon the above mentioned and Code of Misdemeanour Procedure [7] § 29 (1) 1), the Data Protection Inspectorate decided not to begin a misdemeanour proceeding, since the failure to establish the restriction on access as prescribed by law is not stipulated as a misdemeanour liability in the Public Information Act. The necessary elements of a misdemeanour offence can only be assumed by the holder of information. In this case the holder of information is an agency, not the preparer of the document.

Committee on Decorations

On 10 February 2006 a misdemeanour notice was sent to the Data Protection Inspectorate by the Committee on Decorations on the basis of AvTS § 38 (3). Pursuant to the notice, the weekly newspaper "Eesti Ekspress" had disclosed extracts from the 12 January 2006 application presented to the Committee on Decorations for the awarding of decorations, which had been designated for internal use, pursuant to AvTS 35 (1) 11). Pursuant to the above mentioned provision, the holder of information was obligated to declare the notice, which contained personal data, as intended for internal use, if this would significantly jeopardise the inviolability of the data subject's private life.

Pursuant to IKS § 4 (2) the following are private personal data:

5) data revealing details of family life;

6) data revealing an application for the provision of social assistance or social services;

7) data revealing mental or physical suffering endured by a person;

8) data collected on a person during the process of taxation, except data concerning tax arrears.

Based on this, the necessary elements for an offence prescribed by AvTS §54[1] (1) were not met, and therefore a basis was missing for the further continuation and the instituted proceeding was subject to termination pursuant to Code of Misdemeanour Procedure § 29 (1) 1).

[7] RT I 2002,50,313; 2002,110,654; 2003,83,557; 2003,88,590; 2004,46,329; 2004,54,387; 2004,54,390; 2004,56,403; 2005,39,308; 2005,40,311; 2005,71,549; 2006,21,160; 2006,31,233; 2006,31,234; 2006,48,360; RT III 2004,9,96.

Based upon the above mentioned and directed by Code of Misdemeanour Procedure § 29 (1) 1), the inspectorate terminated the misdemeanour proceeding No 2.1-21/06/01. Regulation prepared on 2 May 2006.

This was followed by 26 June 2006 precept No 2.1-9/06/10 issued to the Committee on Decorations by AKI, since in the course of the surveillance performed for the Public Information Act is was discovered that the State Secretary had, pursuant to AvTS 34 (2), established with his directive No 12 of 4 February 2005, based upon § 35 (1) 11) of the above mentioned act, a restriction on access to the application for submitted to the Committee on Decorations for the awarding of decorations, which had been designated for internal use.

Pursuant to the above mentioned provisions, the holder of information is obligated to declare the notice, which contained personal data, as intended for internal use, if this would significantly jeopardise the inviolability of the data subject's private life.

Pursuant to the § 9 (1) of the Decorations Act[8], the President of the Republic awards decorations to the Estonian state and people for performed services in accordance with legislation to both Estonian citizens as well as foreigners. A military unit can be awarded decorations for combat services. The description of the above mentioned services does not require the communication of any private personal data – "For services performed on behalf of the Estonian state and people" requires that it does not involve data which can cause significant damage to private lives.

The form "Application form for awarding Decorations" forwarded by the Committee for Decorations to AKI during the course of the misdemeanour proceeding No 2.1.2.1/06/01 and approved by Government of the Republic regulation No 68[9] of March 1997, does not foresee that it requires the inclusion of data which may significantly damage a persons private life. The inspectorate did not agree with the position of the Decorations Committee presented in misdemeanour proceeding 2.1-2.1/06/1, pursuant to which the private life of a person could be damaged by the decision not to award a decoration or the reasons behind such a decision. This involves the awarding of decorations, which are given for services provided for the welfare of the Estonian state or society. State decorations are not awarded for an exemplary private life, the marking of which in the application could suffer, in the event of disclosure, significant damage.

State decorations are not a mark of the Decorations Committee or the Presidents personal sympathy, but instead a recognition by the Republic of Estonia. As a result of this, the reason for

[8] RT I 1997,1,4; 1998,47,699; 2001,43,240; 2002,63,387.
[9] RT I 1997,28,430; 2005,71,559.

the awarding of the state decoration cannot be a source of significant damage to private life, and society has a right to know why the person was honoured. Society has the same right to know based on which reasons a person who is submitted to receive a state decoration is deemed by either the President or Decorations Committee to be unworthy of receiving the decoration.

Thus, the decision of the Decorations Committee was not justified in applying a restriction on access to the completed "Application forms for the awarding of Decorations" with the reason being that if the information would be disclosed it would significantly damage the inviolability of the data subjects private life.

AKI issued the precept to the Decorations Committee: to remove the illegal restriction on access to the completed "Application forms for the awarding of Decorations" presented to the Decorations Committee.

National developments in the field

The Data Protection Inspectorate considers the development of the area on a national level to be critical. Our officials participate, within limits, in various national workgroups, for example e-health and infectious disease observation workgroups, e-file biometric workgroup, etc.

Amending of IKS and AvTS

The wording of the valid Personal Data Protection Act entered into force on 1 October 2003. The objective of the draft act prepared by the Ministry of Justice in the current year is to repair some tight spots which have appeared during the implementation of the law.

Since at the time of its preparation IKS was based upon the European Parliament and Council Directive 95/46/EÜ regarding individual protection in the processing of personal data and the free movement of such data, then the current years draft legislation has also primarily preserved the principles of the valid legislation, which are specified, if necessary, and harmonized in their wording.

AvTS entered into force on 1 January 2001. The need for the amendment of the legislation stems, above all, from the circumstance that over the period of five years developments have occurred in society, with which the law needed to be brought into conformity with and at the same time problems have occurred in the implementation of the law, which the draft legislation attempts to resolve. The objective of updating the AvTS rests, above all, in increasing the transparency of public power.

International cooperation and development

In the current year inspectorate officials have taken part in several yearly and inaugural international conferences and workshops, where topics that are continuously in development were discussed as well as new development directions in the data protection field. Listed below is a short overview of the more important events and topics.

The main topic of the yearly European data protection supervisory agency spring conference (Budapest) was personal data processing in historical as well as scientific investigations, state field of health databases, genetic data (AKI director general presented a report on Estonia's Gene Bank and its current state) and under discussion as newer development directions were *whistleblowing* (notification of internal misdemeanour conduct), geolocalisation and RFID technology (RFID – *Radio Frequency Identification)*.

They also participated in the conference "Public security and personal data protection" (Poland), where the connections between processing and public security were reviewed, discussed Schengen II generation information systems processed personal data end-use and also talked about the possible development of the surveillance community.

Central and Eastern European personal data protection representatives as the eighth conference (Bulgaria) exchanged monitoring performance experiences and debated current events topics (public awareness, political advertisement, freedom of speech, video surveillance and the Schengen information system).

During the accounting period the Inspectorate's officials have participated in practical workshops, the goals of which were the exchange of direct work experience and training and stepping up cooperation.

In March of the current year, the European Union data protection supervisory agencies *Case Handling Workshop* took place in Madrid, where the main topics were: personal identification documents and unique personal identifiers, public e-services, data protection at work, personal data protection and public notification.

The working meetings of the telecommunication fields international data protection work group (IWGDPT) have taken place twice during the given period (in April in Washington and in Berlin in September). The main emphasis of both conferences was personal data processing through telecommunications and technology development. Special attention was given to VoIP (*Voice*

over IP) as well as electronic health data, radiofrequency detection, spamming and cross-border marketing.

The Inspectorate is also participating in the INTERREG IIIc e-PPRODAT[10], the objective of which is the development of already in use and to be developed in the future public e-service development data protection through cooperation work between supervisory agencies and public organisations.
The project began in February 2005 and the planned term for completion is February 2007. The participation of the Inspectorate in the project has intensified considerably in the current year. Among other things, on 29 September a working meeting of the project's management committee took place in Tallinn, and during the disclosure period for the report, also in progress at the Data Protection Inspectorate, is the disclosure of the Estonian language project book.

The Inspectorate is continuously active in several European Union workgroups. The more important of these groups is the data protection workgroup which was created based upon Directive 95/46/EÜ article 29, the joint supervisory agency (Europol JSB) created on the basis of Europol convention article 24, the joint supervisory agency (Schengen JSA) created on the basis of Schengen convention article 115, and the joint supervisory agency (Customs JSA) based upon article 118 of the Convention on the use of information technology for customs purposes.

Article 29 data protection workgroup

Article 29 data protection workgroup meets regularly 5 times per year, the work group was created with the objective of providing recommended instructions and positions and is not involved in any supervision work. Work group members are all European Union member states data protection supervisory agencies and the European Data Protection Supervisor, as also take part in meetings with other European state data protection representatives.

The topics under detailed discussion in the work group cover, to a great extent, topics presented at various conferences. The more important positions given by workgroups in the current year are related to the following topics: *whistleblowing*, e-mail filtering service, electronic communications services and data preservation, infectious disease prevention and gathering of data concerning travellers (USA), opinion regarding the European Courts 30 May 2006 decision related to the forwarding of traveller data (PNR), questions regarding the child maintenance obligation, use of site data.

[10]Projekti kodulehekülg: http://www.eprodat.org/

Europol's Joint Supervisory Body

Europol JSB of the Europol Joint Supervisory Body's objective is in conjunction with the Europol Convention to monitor Europol's activity, ensuring the rights of individuals in data storage, processing and use. The joint supervisory body's competency also includes the review of questions regarding the performance of Europol's personal data processing and use operations, review of questions involving independently conducted monitoring by member state's supervisory bodies, review of questions regarding the right to receive information and the finding of resolutions for problems that come to the forefront and the disclosure of positions on their basis.

During the accounting period the Europol joint supervisory body inspection work group performed the annual Europol and Europol information system (EIS) inspection. The conformity of Europol's operations with the convention and the legislation, implemented security methods, etc., approved on its basis. Europol's joint supervisory body inspection work group prepared an extensive report about the inspection results, which was sent to Europol for the publication of results and/or consideration. Selected from the report were some more important topics, to which national surveillance agencies should definitely pay attention to during the inspection of national units.

During the accounting period several changes occurred in the work of Europol. In close cooperation with the joint supervisory agency Europol's Administrative Board changed the procedure for opening Europol's analytical work files (AWF). As well as several other Europol convention provisions. The joint supervisory body prepared an opinion regarding all of the changes.

During the accounting period Europol's future was discussed, namely the Council of the European Union is planning to replace the Europol convention with a decision of the council. This draft legislation was also under discussion at the joint supervisory agency meeting. Concerning the draft legislation, the regulation affecting the joint supervisory agency will remain largely the same, with the addition of cooperation between the European Data Protection Supervisor (EDPS), since Europol will begin to cooperate with OLAF (The Commission of the European Communities Anti-Fraud Office), CEPOL (European Police College), Frontex (European Agency for the Management of Operational Cooperation at the External Borders) and the European Central Bank, which are all under the supervision of EDPS.

Customs Convention join supervisory agency

The Data Protection Inspectorate is also participating in the work of the Joint Supervisory Authority (JSA) for the Customs Information System. The joint supervisory agency has the authority to perform supervision of the Customs Information System, to review the implementation or interpretation questions related to this work, to investigate problems, which occur in member states national supervisory agencies independent of the performance of the supervision or the use by individuals of permission to access the system, as well as preparation of offers for the joint resolution of problems.

Like all other supervisory agencies, the Custom Convention's JSA also performed during the accounting period the joint yearly inspection of the Customs Information System (CIS) centres and the inspection report was sent to OLAF for the publication and/or consideration.

Based on the results of the central units inspection results, a questionnaire was prepared, which was the basis for joint inspection of CIS. The questionnaire was forwarded by national supervisory agencies to their national CIS using authorised agencies and the joint supervisory agency consolidated report is based upon their answers, which will be discussed at the December 2006 meeting.

Schengen Joint Supervisory Body

The Data Protection Inspectorate is participating as an observer in the Schengen JSA work. The joint supervisory agency is responsible for the supervision of the Schengen information systems technical support unit. The joint supervisory agency also has the authority to review questions related to the implementation or interpretation of the Shengen Information System, to investigate problems, which may occur in convention members national supervisory agencies independent of the performance of supervision or the use by individuals of permission to access the system, and to prepare harmonised proposals for the joint resolution of present problems.

During the accounting period Schengen's joint supervisory body prepared its seventh activity report about its own activities, which reflects the joint supervisory body's activity from January 2004 until December 2005.

A joint inspection was carried out pursuant to article 99 of the Schengen convention or the Schengen information system (SIS), regarding covert surveillance of persons or automobiles or the joint inspection of notices entered regarding special audits, the results of which were prepared as a report.

An opinion was prepared on the interpretation of Schengen convention article 114 or in other words regarding the national supervisory agency's obligations and authority. In short, it is the national supervisory agencies responsibility to control that:

- the entered data (alert) corresponds to the criteria of the convention (article 105; 109-111; 112);
- the terms and conditions regarding the permissibility of the data entered conform to national legislation (competent authority's legitimate and valid decision);
- entry of data (alert) must be important and justified. This condition arises from convention article 94 (1) "The convention participant that submitted the notice makes sure that the importance of the incident justifies its entry into SIS)".

Thus, national supervisory agencies must have sufficient competence, rights and opportunities for controlling the conformity of the above mentioned criteria for the entry of data.

The new legal basis for the current draft legislation for SIS II was thoroughly debated as well as the performance of supervision over SIS II.

European Union data protection supervision authority Police Working Party

The working group prepared the European Union data protection supervision authority joint position European Community third pillar data protection instrument (Council of Europe framework decision on the protection of personal data processed in the framework of the police and judicial co-operation in criminal matters (COM 2005 475)) regarding the final version. The main problem is the scope of application of the framework, if framework requirements should be applied to processing of personal data by national law enforcement authorities, and not only in the framework of cooperation between member states regarding personal data exchanged between national law enforcement authorities. At the November 2006 meeting of the European Union data protection supervision authority managers, a declaration was prepared, pursuant to which all law enforcement authorities support the application of the European Unions data protection supervision authority framework for the processing of all law enforcement agencies personal data.

Schengen data protection evaluation commission

The Republic of Estonia, upon joining the European Union, took it upon itself to join the Schengen convention and its Additional Protocols. The objective of the Schengen agreement is

the free movement of persons in the Schengen area. In everyday life it is comprised of no checks at the common borders of member states and the possible negative effects resulting from the reduction of controls is reduced by the of compensation methods. Compensation methods are the Schengen information system, strengthened controls on external borders, monitoring of foreigners, cross-border cooperative police work and a common legal environment.

The assignments of the Data Protection Inspectorate related to the Schengen judicial area are related, above all, to the Schengen information system. The objective of the information processed by the Shengen information system (SIS) is to aid the law enforcement authorities in the Schengen judicial area in ensuring public order and security. The inspectorates tasks are the independent supervision of the national part of SIS regarding data file entry and control over the fact that the processing and use of entered data does not violate the rights of the person concerned.

The Republic of Estonia (and the inspectorate) preparation for joining the Schengen information system was evaluated by an expert group on 21-22 September 2006. At the time of the report's publication, the Council of Europe has with its decision evaluated the need for carrying out the repeated evaluation of the data protection field, so that the recommendations and instructions in the evaluation commissions report are implemented before joining the Schengen information system.

AKI's plans for the following period

In the following time period AKI is planning an increase at its own initiative in the volume of supervisory operations. The objective is ensuring the legitimate performance of obligated subjects. In order to achieve this an analysis of the current administrative training and penalty policy is planned, development of good administrative practices and, among other things, the raising of administrative capacities.

The keywords for the following year are also the raising of general awareness and development of cooperation between state and local government authorities. The objective is to provide persons with the opportunity to implement their rights and provide the processors and holders of information with the knowledge to improve the performance of the implementation of obligations.

Pursuant to the desire to raise the level of awareness we have already started and are planning to continue on a larger scale with lectures for upper secondary level students in general education schools in the field of data protection.

AKI is planning to hold a conference on 28 January of next year, within the framework of the International Data Protection day, to discuss e-society and data protection related topics. In the framework of the event we are waiting for specialists and parties interested in the field to speak and participate in the discussion.

The field may be highlighted separately with keywords, which have risen during the current period: e-Health, Gene Bank, educational institutions; creation and amendment of corresponding regulations, monitoring of their development directions and active participation in the process.

SUMMARY

The Personal Data Protection Act entered into force on 19 July 1996, and the personal data protection field regulation has now been valid in the Estonian judicial area for 10 yeas. The inspectorate confirms that the so-called adjustment period is beginning to end and the personal data processors have had sufficient time to get used to the requirements arising from the regulation or in other words to implement the requirements in their work. Therefore, AKI is toughening its administration training and penalty policies in the case of significant violation of processing requirements.

Even so, the inspectorate must in its continued activity find a suitable balance between its deterrent activities and its supervisory activities. Its deterrent activities include in itself both the raising of citizens awareness as well as participation in various work groups and giving opinions regarding draft legislation.

The raising of general awareness in deterrent activities is very important, since the carrying out of training by AKI officials helps in the understanding of the nature of the field and the resulting obligations and requirements for both data processors as well as subjects. At the same time, it is possible for the inspectorate in its everyday work to concentrate on condensed areas of specific fields, which have appeared from information gathered during training.

We also hold the providing of opinions regarding various draft legislation to be a significant activity. This type of activity guides the composers of legislation and the attention of recipients to circumstances, which at first glance appear to be unimportant, but which may from one side exceed a persons fundamental rights and freedoms and from the other side apply for information holders and personal data processors excessive and expensive obligations.

Becoming a full legal member of the European Union included the significant growth in the volume of work for the inspectorate, performing the supervisory obligation for a Europe wide information system (Europol, Schengen, Eurodac etc.). The developments of the corresponding field at the European Union level provide an indication of the increase in the exchange and centralisation or information (VIS, biometrics, etc.).

NOTE 1

	2004.a	***2005.a***	***01.10.2005-30.09.2006****
Giving of opinions regarding draft legislation	50	48	39
Training	15	30	34
Registration			
Total number of registration applications:	390	368	414
including first time applications			103
including repeat applications			241
including applications with changes			70
Issued sensitive personal data processing licences	314	361	229
Refusals	76	29	2
Left unreviewed			2
Precepts			4
Warnings			3
Penalty payments			2/18000.-
Giving of opinions to data bases	40	16	9
Monitoring			
Total on-site monitoring:	35	28	48
1) National control	35	28	47
including as a result of required proceedings			18
including self initiated	8	8	29
2) International/EU	-	-	1
including as a result of required proceedings	-	-	-
including self initiated	-	-	1
No deficiencies were discovered			13
Deficiencies discovered			36
including precepts			7
Opinions regarding readiness for processing			374

Procedure			***IKS***	***AvTS***	***AKS***
	2004 total	***2005 total***	***01.10.2005-30.09.2006***	***01.10.2005-30.09.2006***	***01.10.2005-30.09.2006***
Explanations, memoranda challenges and complaints	61	81	110	99	1
No violations were discovered			95	86	1
Violation was discovered			15	13	-
including precepts	7	9	3	5	-

including misdemeanours	5	5	10	8	-
Fines and periodic penalty payments			9/58800.-	-	-

*The internal statistical format changed at the beginning of the current accounting period

The Data Protection Inspectorate presents a report each year on 1 December, to the Riigikogu Constitutional Commission and the Chancellor of Justice, pursuant to Personal Data Protection Act[11] § 41 (1) and Public Information Act[12] § 54 (1) regarding circumstances related to the performance and implementation of Acts.

The Data Protection Inspectorate's main area of activity is the implementation of the independent supervision over the legality of processing personal data and keeping databases, as well as organizing data protection activities and the performance of other tasks arising from or based upon legislation.

Members of the reporting group included: Gina Kilumets (Head of Development- and Analysis Department), Maarja Kirss (Development and Analysis Department Adviser), Stiina Liivrand (Development and Analysis Department Adviser), Merit Vaim (Head of Supervisory Division), Rainer Kivisäk (Head of registration division) and Taago Pähkel (Head of Proceedings Division).

[11] RT I 2003, 26, 158; 2004, 30, 208
[12] RT I 2000, 92.597; 2002, 61,375; 63, 387; 2003, 25, 153; 26, 158; 2004, 81,542; 2005, 39, 308