INTRODUCTION

1. Goals and functions of the agency

The Data Protection Inspectorate protects everyone's constitutional rights:

1) the right to obtain information about the activities of agencies and officials;
2) the right to inviolability of private and family life in the use of personal data; and
3) the right to access the information collected about them.[1]

We are authorised to do this by:

1) the Personal Data Protection Act:
   - the obligations of personal data processors;
   - everyone's rights with respect to their data;
2) the Public Information Act:
   - everyone's right to obtain public information;
   - adherence to restrictions on access;
   - control over public sector databases;
3) the Electronic Communications Act:
   - protection from unsolicited direct marketing by electronic channels; and
4) international legislation:
   - joint supervision over cross-border databases and other international cooperation.

In order to perform these functions, we act as:

1) **an educator and consultant:**
   - responding to requests for explanations; helpline;
   - counselling (especially with regard to products and services of significant impact);
   - training; media notification;
2) a **designer of legal practices:**
   - guidelines at the national level and in international cooperation;
3) a **policy adviser:**
   - counselling on legislative drafting and information systems of the public sector;
   - planned and extraordinary presentations to the Constitutional Committee of the Riigikogu and the Chancellor of Justice;
   - participation in national and international advisory bodies;
4) an **ombudsman:**

[1] The right to obtain information about the activities of agencies arises from subsections 44 (2) and (4) of the Constitution. A person's right to access the information collected about them arises from subsections 44 (3) and (4) of the Constitution, but it does apply to the public sector only. European Union law extends this to other sectors as well. The right to inviolability of private and family life arises from § 26 of the Constitution and also covers the collection and use of data about persons. A person's control over the data that concern them i.e. their informational right of self-realisation related to the right to free self-realisation stipulated in § 19 of the Constitution. The right to inviolability of personal life related to the right to confidentiality of messages stipulated in § 43 of the Constitution.

- we resolve complaints and challenges, and verify facts in the course of state supervision where necessary;

- we initiate supervision ourselves in the event of suspicions;

- we issue legally binding precepts and decisions on challenges;

5) an **auditor and a licensor**;

- compliance and adequacy audits (incl. audits of cross-border databases);

- comparative monitoring (incl. monitoring of cross-border databases);

- processing and registration of sensitive personal data;

- co-ordination of public sector databases;

- granting permission to use personal data for scientific research without the consent of data subjects;

- granting permission to forward personal data to foreign countries with insufficient personal data protection levels; and

6) an **enforcer and a punisher**:

- imposing penalty payments;

- in emergency situations, we apply security measures ourselves at the expense of the personal data processor;

- extra-judicial misdemeanour procedures.

2. Activity statistics

Our activities in recent years are partially illustrated by the following table:

	Sensitive Personal Data Processing Register		**Explanation requests, demands and memos, requests for information**	**Calls to helpline**	**Challenges, complaints**	**Administrative coercion and punishments for misdemeanours**			**Approval of public sector databases**
	notification applications	precepts				precepts	Misdemeanour procedures (completed)	fines, penalty payments	
2010	468	50	893	1061	592	153	35	15	136
2009	1429	459	944	851*	306	49	46	12	265
2008	960	210	679		358	37	23	14	91
2007	629	106	251		110	35	4	2	11

*we launched the helpline in March 2009

The volume of explanatory and counselling work (requests for explanations; helpline) has stabilised compared to indicators from the previous two years.
However, the number of complaints and challenges has doubled. In our opinion, this increase has not been caused by a sudden deterioration in the area of information law, but the fact that people are better informed about their rights.

The number of precepts has almost trebled due to the increase in the number of complaints and challenges as well as the new form of supervision – comparative monitoring. Tens or hundreds of objects of monitoring are reviewed in one monitoring session and we react to serious omissions with proposals and precepts. We launched three monitoring sessions in 2009 and completed six such sessions in 2010.

Compliance and adequacy audits are also a new form of supervision, and we initiated four audits in 2010. These audits give us a comprehensive picture of the compliance of large and sensitive information systems with personal data protection requirements. We use international methodology to conduct these audits.

Notification of sensitive personal data processing moved largely to the Internet at the end of January 2010. Automatic error filters and the standard forms based on the submitted type make it easy for both the submitter and the receiver. The precepts issued to those who ignore the registration obligation are also standard. This is why we transferred the notification to our administrative department, as it allows our main departments to focus on more specific work.

Last year we issued five personal data protection and public information guidelines and participated in the preparation of nine opinions via the common workgroup of European data protection authorities.

The agency's budget was 8,624,255 kroons. There are still 18 positions covered by the salary fund. The rate of staff turnover decreased – 2 colleagues left the agency. There were no significant structural changes.[2]

3. Activity methods

The scope of personal data protection covers all sectors of society. It also covers all private persons who process the personal data of others outside of the private sphere (e.g. on the Internet). All institutions and also all persons in private law that perform public functions or use public funds are possessors of public information.

There is the constant threat – considering the total number of potential objects of supervision, the small number of staff we have and the increase in the amount of work placed on the 'conveyor belt' – that we will not be able to see the wood for the trees.

[2] Two of the main departments deal with personal data protection and public information issues. In order to improve competence, one of them specialises in 'soft' areas of life (e.g. ordinary business, education and the social sphere and the Internet) and the other in 'hard' areas of life (e.g. security, legal protection, finance and statistics). The administrative department provides support services, registers cases where sensitive personal data are processed and organises communication with the public. As we are first and foremost a legal authority, our Chief Legal Officer reports directly to the Director General.

So how can we be influential in our area of responsibility regardless of our quantitative indicators? The first thing we did was to accelerate the 'conveyor belt' of reacting activities (registration, requests for explanations and review of complaints) in order to increase the scope of supervision on our own initiative and other proactive activities. This includes:

1) from 2008 to 2009, we launched a major action to call processors of sensitive personal data to comply with the notification obligation, which means that less supervision is required in this area and the notification conveyor belt moves quickly with the help of online proceedings and does not create much burden for us;

2) the helpline cuts our workload, as answering simple questions by phone is less time-consuming than correspondence;

3) we introduced a simplified supervision procedure with regard to less complicated problems; and

4) we use risk-based gradation of measures when we react to breaches.[3]

Getting the volume of work that lands on our desks or reacting work under control allows us to act as a strategic regulator:

1) we intervene on our own initiative where risks are higher and intervention has a greater impact;

2) we use new forms of supervision: extensive comparative monitoring and audits that allow us to see the big picture;

3) instead of 'retail training', we focus on the preparation of guidelines and 'wholesale training';

4) we improve the efficiency of cooperation; and

5) we improve the efficiency of our media work.

4. Improved adherence to the Public Information Act

The monitoring conducted in 2009 and 2010 indicated that there were gaps in adherence to the Public Information Act, which entered force at the start of the previous decade. The requirements established for the websites and web-based document registers of institutions by law were ignored on a large scale. There was no consistency in the interpretation of the act (especially in the implementation of access restrictions regarding information) or in the structure of web information in the public sector.

There are many reasons why we found ourselves in such a situation. First of all, nobody owned the subject of public information at the state level. The situation was often also the same at the level of institutions where people tended to regard public information requirements as an annoyance that got in the way of their principal activities.

[3] Gradation from easier to more difficult: recommendation (feedback not demanded); proposals (feedback demanded); precept; penalty payment; misdemeanour procedure.

Secondly, the lack of ownership meant that any training that was given was insufficient and there were no guidelines.

The third reason is the situation whereby every administrative agency and local government is forced to develop similar information systems, incl. document registers and websites, independently. This results in a waste of resources and inconsistency that makes things difficult for users. Information about the state of Estonia and its public sector is presented on the Internet considerably more inconsistently than similar information on larger states.

The fourth reason is that supervision of the adherence to the Public Information Act is mainly based on complaints, which proved clearly insufficient when problems started mounting up.

Monitoring allowed us to map the situation, obtain feedback and start to develop guidelines. We discussed the relevant drafts at several roundtables and training sessions. On 17 May 2010 we published the General Guidelines of the Public Information Act for institutions, which was followed by the publication of the abridged Special Guidelines for public information holders in private law on 16 June 2010.

The proposal made to the State Secretary regarding the determination of the owner of the subject of public information and adherence to the relevant act resulted in the amendment of the Common Bases of Operations Procedure (subsection 3 (3)) on 4 November 2010. It assigned to governmental agencies the obligation to appoint the person who is responsible for organising the publication of documents and protection of the personal data contained therein in the agency as a whole. This circle of persons overlaps largely with the document management executives of agencies. According to the regulation issued by the government, these persons must coordinate the relevant activities in the various departments of their agencies.

We organised extensive training for the representatives of state agencies and local authorities with the help of the Ministry of Finance and the State Chancellery, which was based on the General Guidelines of the Public Information Act.[4] The persons sent by state agencies to these training courses are presumably the same persons who will be in charge of adherence to the Public Information Act.

We are planning to cooperate with the State Chancellery to include the persons who organise adherence to the Public Information Act in central agencies in the network of document management executives of ministries that is already functioning. This network could make adherence to the Act more consistent and give effective feedback about any implementation problems.

We are planning to launch the development of the privacy policies of agencies with the help of the network. As an example, we prepared the privacy policy of the Data Protection Inspectorate How Do We Keep Information about Your Private Life? and published it on our website on 13 October 2010.

The harmonisation of web information in the public sector is based on the amendment regarding the information portal of Estonia made to the Public Information Act (§ 32^1), which was developed with

[4] Ten two-day training sessions in total, incl. three in 2010 (for state agencies) and seven in 2011 (for municipal, city and town governments).

our assistance and entered force on 28 December 2009. The information portal www.eesti.ee has existed for more than ten years, but the web information of agencies is not interfaced to the portal. There is no cooperation in its content management in the public sector.

In cooperation with the Estonian Informatics Centre, we organised two training days for persons who deal with web information in agencies (27 August and 10 September 2010). We proceeded from the need to create a network of the people who are responsible for web messages in agencies. We hoped that the training would give the extra push needed for the creation of this network.

Unfortunately, I must admit that the legal provision (§ 32^1 of the Public Information Act) concerning the Estonian information portal has not had any significant impact. There was still no implementing regulation at the time this text was written. We need an implementing regulation to stipulate the exact obligations of public information holders with regard to the information portal. Without this, there will be no cooperation between the small central office of the information portal and all other agencies.

5. Private life in employment relationships

The issue of the personal data of employees was our priority in our proactive activities concerning personal data protection in the previous year. This covers the collection and use of the data of jobseekers, employees and former employees, and background checks concerning employees.

The legal foundation for this does exist. The Employment Contracts Act stipulates that an employer who prepares an employment contract may only ask a person for information with regard to which the employer has a legitimate interest (§ 11). During the employment relationship, the employer must respect the privacy of employees and verify the performance of their duties in a manner which does not violate the employee's fundamental rights (clause 28 (2) 11) of the Employment Contracts Act). The Personal Data Protection Act stipulates the general principles (expedience and minimalism; see § 6).

However, these are just the general principles. When we started a discussion about their implementation in real life, the only more or less clear and unanimous opinion was that employees may not be observed on camera in toilets and shower rooms.

Hundreds of practical questions were raised in the course of the discussion – how can the background of jobseekers and employees be checked, who may read e-mail messages containing the employee's name and the employer's domain name, how to check the health of employees etc.

There were also disputes about fundamental issues of the theory of law. For example, when does an employer process the personal data of an employee on the basis of the latter's consent (as we all know, consent may be withdrawn) and when is it done to guarantee performance of the employment contract.

The data protection agencies of several countries have prepared short and simple guidelines about the rights and obligations of employers and employees. We wanted to do the same. Unfortunately, we found that it was out of our reach, as there was no basic legal analysis in Estonia. Legal literature

only covered a few aspects and national court practice offered even less. There was no legal foundation on which we could build our simple summary.

We discussed the subject of protection of private life in employment relationships at our annual conference on 27 January 2010 and later at a roundtable for employers and central employee organisations which was attended by other agencies and experts. Personal Data Processing in Employment Relationships was at last ready for publication on 24 January 2011.

Monitoring of video surveillance of employees was also covered by the subject of personal data processing in employment relationships.

6. Personal data protection and databases

The more sensitive the information contained in a database, the stronger the internal control measures that the keeper of the database must apply regarding the use of such information. For example, internal control of the use of the Population Register is relatively efficient. We are informed of any suspected cases of misuse.

Management of information assets, incl. granting of access rights, was centralised in the Police and Border Guard Board after the merger of the agencies, and the internal control system of the merged agency was made more efficient. I advise other agencies that keep large, sensitive databases to look into the implementation of a similar model.

Zero tolerance was established with regard to persons who misuse the police database, and anyone doing so is punished with disciplinary as well as misdemeanour procedures. There is regular information exchange between the police and ourselves for this purpose. This has brought about a noticeable change for the better within the organisation.

Once the problem of archiving and deleting outdated data finds a satisfactory solution, we will be able to say that the biggest risks relating to the police database have been minimised.

We also wanted to launch cooperation in the area of e-health similar to the internal control of the Population Register and the police database. However, the relevant agreement so far only exists on paper, as there is no supervision model in e-health.

We did conduct separate monitoring of the registers of residents created by local authorities on their own initiative. Local authorities are the local keepers and users of the National Population Register. Several local authorities, however, still keep additional local registers of residents without having any legal basis for doing so. We issued precepts requiring their closure.

7. Other important issues of personal data protection

Requests for explanations and complaints about unlawful disclosure of payment defaults and debts have been a growing segment since 2008. Even the fact that our legislation, which permits disclosure of payment default data without the person’s consent in the interests of transaction turnover, is among the most liberal in Europe.

We have issued guidelines regarding disclosure of information about payment defaults and debts (Disclosure of Payment Defaults, published on 2 February 2010), given information and issued precepts, and imposed misdemeanour punishments.

An even larger number of requests for explanations and complaints relate to search engines and communication environments. The problem of insufficient awareness about the Internet emerges far too often. People fail to understand that search engines only reflect data on websites *("Remove my data from Google!").* People keep posting their data on websites opened by search engines. They do not understand that uploading photos and details of other persons is impolite and illegal, and may lead to criminal liability.[5] Unfortunately, I have to admit that the practice and motivation of police officers to investigate identify theft is sometimes insufficient.

We conducted comparative monitoring of the terms of use of social networking environments, and made proposals and recommendations to their administrators.

I am embarrassed to say that our state itself keeps outdated information that is damaging to people on the Internet where it can be accessed by search engines. I am talking about the official publication *Ametlikud Teadaanded*. It is web-based and can be googled. Every type of notice is published for a reason, and this passes in time. However, there is no deadline until which these notices remain public. A court summons or bailiff's notice remains on the Internet for years. It stays there even if the person is cleared of any wrongdoing. We found that this situation could not have been intentionally created and it was a gap in legislation. This is why we are having outdated notices removed on the basis of complaints, until permanent legislation is established. Reacting to complaints is of course a temporary solution.

I found the problem of *Ametlikud Teadaanded* so serious that I used the right to present an extraordinary report to the Constitutional Committee of the Riigikogu and made suggestions on how to solve the problem. This was not my only extraordinary report – I presented another regarding the draft amendment of the Political Parties Act (516 SE). I am pleased to say that the legislator accepted the suggestions made in both reports.

Our regulation of electronic direct marketing was insufficient and in conflict with European Union law. I commend my colleagues from the Ministry of Economic Affairs and Communications for the relevant amendments to the Electronic Communication Act and the Information Society Service Act. These entered force on 10 July 2010. The amendments have given us a better legal basis for handling electronic advertisements (especially in e-mail and text messages) that disturb people. We are trying to deal with the biggest spammers preventively in order to reduce the number of complaints.

§ 16 of the Personal Protection Act permits us to organise scientific research without the consent of the examined persons in certain cases; only the permission of the Data Protection Inspectorate is required. Use of this provision really took off last year. We are of course cautious about giving such permission. It usually concerns the need to merge personal data from different databases (e.g. from health-related databases) for the purpose of research. Merging data means that the person who issues the data cannot de-personalise them, as otherwise they could not be tied to data from other

[5] Identity theft is punishable pursuant to § 157.2 of the Penal Code.

databases. We admit that our permission really is not the best solution. It was stated in the draft of the current Personal Data Protection Act, which entered force in 2008, that it is essential to create a common coding centre which would guarantee a convenient de-personalisation service for researchers.

The initial draft of the new Official Statistics Act adopted last year restricted the use of data for scientific research considerably more than the Personal Data Protection Act. The draft was amended and the requirements were relaxed on the basis of our suggestions.

Cooperation in the common workgroup of data protection agencies created by the European Commission was rather successful last year. The opinions I would like to highlight concern the following issues of important pan-European guidelines: a) applicable law (the situations in which the data protection laws of one or another country must be implemented); b) radio-frequency identification (RFID); c) behaviour-based Internet advertisements and collection of data for this purpose; and d) determination of data controllers and processors. We approved the code of conduct of FEDMA, the European direct marketing organisation, for its members. The adopted documents are available on the workgroup's website.

Working in the area of personal data protection and public information is exciting, but stressful. We must find a way to tie our two areas of work with all other areas of life – social and police work, social networking environments and e-business, banking and statistics – whatever they may be. We must keep up with rapid social and technological development and know how to prevent problems. In our role as the ombudsman, we have to make decisions that are right and fair whilst proceeding from legal notions that may be interpreted in different ways (public interest, excessive damage etc.).

I would like to thank my colleagues for the achievements and success described herein, and also for those that did not make it into the report.

Our small agency would not be able to perform its functions successfully if it had to do so alone. I am grateful to everyone who took part in the roundtable and all of our excellent partners.

Viljar Peep,

Director General of Estonian Data Protection Inspectorate