Summary by the Director-General

Pursuant to the Personal Data Protection Act and the public sector information Act, I am submitting an annual report regarding the performance of both Acts, to the Constitutional Committee of the Parliament of Estonia, and to the Chancellor of Justice. In addition to the review, I am also providing an overview of this year's activity plan, and offering my policy suggestions.

I am hereby using the opportunity to wish the new members of the Constitutional Committee and the newly appointed Chancellor of Justice strength and success in their job loaded with great responsibility.

I. Why protect personal data? Why have public sector information available?

Everyone has the right to the inviolability of their family and private life, confidentiality of messages and free self-realisation. All these fundamental rights are jeopardised when personal data is misused.

Misuse may also jeopardise a person's fundamental right to choose an area of activity, profession and workplace. Particularly so if the data concerning the person was collected without their knowledge.

In order for the person to be aware, and be able to protect themselves, they have to have the right to access the information collected about them. However, this or any other rights associated with personal data is not absolute.

By protecting the fundamental rights, we are also protecting public interests. In order for the digital economy and the e-state to develop, we need, among other things, trust. People do not trust databases and e-services if they doubt that the information collected about them is protected therein.

As a rule, authorities collect and use information without the person's consent and sometimes also without their knowledge. Misuse of information by the authority leads to the misuse of power. Lawful use of personal data in the public sector is one of the prerequisites for the sustainability of a democratic state based on the rule of law.

Availability of public sector information is important to a person requiring specific information. But as a whole, this also affects the whole of society. Availability of public sector information helps to ensure more efficient control over executing public authority, using public funds and performing public duties.

Availability of public sector information, incl. as open data in machine-readable form, affects business and innovation.

The more personal data and public sector information (with restriction on access) become digitalised, the more important it is to keep them safe.

II. What is the benefit of the Estonian Data Protection Inspectorate?

The Estonian Data Protection Inspectorate watches over the process of collecting and using personal data and the availability of public sector information. Combining these two different areas of activity into one institution helps to achieve a more balanced approach.

The Personal Data Protection Act is foremost an abstract generic legislation. It is largely based on general principles and the weighing of undefined legal concepts (e.g. public interest, excessive damage).

Their abstract nature and technological neutrality have helped the rules of data protection stand the test of time. This year it will be 20 years since the EU data protection directive 46/95/EC, which the Estonian legislation is based on, came into force.

An institution that bears the name of an inspectorate is usually considered to be a an institution of control, enforcement and penalties. In actuality, 'soft' activities constitute more than half of our work load.

Implementing abstract legal provisions and undefined legal concepts together with the fast development of information society and technology demand that we function as an institution of analysis, prevention and information.

Drafting guidelines is one of our central tasks imposed on us both by the Personal Data Protection Act and the public sector information Act.

Drafting guidelines is particularly important considering the smallness of the Estonian language and legal space. With the help of indicative and explanatory guidelines, we attempt to make up for the shortage of judicial practice regarding the right to privacy, IT laws, and the scarcity of specialised literature (press). The society needs legal certainty.

Rights associated with information are time-critical. The longer the legal proceedings of the violation of rights, the harder it is to capture the information that has leaked into cyberspace. Requested public sector information loses its value to the inquirer due to the long acquisition procedure. For this reason, the Estonian Data Protection Inspectorate has investigative and enforcement powers in matters of supervision, and penal rights regarding cases of misdemeanour.

In our supervisory operations, we are able to use the specific know-how of the Estonian Forensic Science Institute, and the Centre of Registers and Information Systems, if necessary.

In addition to legal proceedings focused on isolated violations:

1) we carry out comparative surveillance that covers tens or hundreds of processors of personal data, or holders of public sector information. As a result of surveillance, we provide generalised positive and negative observations and offer suggestions and recommendations;

2) we organise data protection audits in large and/or sensitive organisations, the main objective of which is to prevent issues;

3) as a new form of procedure, we have adopted circulars, introduced at our own initiative. If there is cause to believe that there is a larger issue regarding the protection of data or public sector information in some area, we will send explanatory circulars to all companies or institutions that may be affected by the issue.

Communication plays a big part in our work – foremost for information activities affecting specific target groups. This also helps us to compensate for our smallness.

The Estonian Data Protection Inspectorate leads or participates in the operation of about ten domestic networks of cooperation and joint working groups as a member or an advisor. Some of these are, for example, the network of public sector information and personal data protection coordinators of governmental authorities, Statistical Council, digital awareness cooperation projects *Smartly on the Web* (Targalt Internetis) and *Smart Security 2017* (Nutiturva 2017), task force for e-health, task force of the Ministry of Economic Affairs for open and link information.

The advisory council of the Inspectorate comprises experts whom we consult in issues regarding priority activities and draft guidelines.

All these measures and forms of cooperation enable us to address not just the individual trees, but the entire forest, to put it figuratively.

III. Protection of personal data and availability of public sector information is not just an Inspectorate matter

The collection and use of personal data is a horizontal topic that includes all sectors of society. Access to public sector information is a horizontal topic that includes whole public sector. The Estonian Data Protection Inspectorate that supervises both of these horizontal topics employees 18 officers. In terms of the size of our staff, we are the second to last governmental authority.

Does that really allow us to efficiently ensure the protection of personal data and the availability of public sector information? Certainly not, if both topics were addressed by the Estonian Data Protection Inspectorate alone and in their entirety.

With respect to personal data, the most important part is the ability of people to check for themselves what information has been collected about them, and how this information is being used. Many public sector databases and e-service environments of the business sector allow for direct access to a person's private information without a separate request.

With respect to the availability of public sector information, too, the awareness and demand of persons requesting and using the information is important.

The Law Enforcement Act that entered into force on 01 July, 2014, establishes clearer bases for drawing intervention limits to supervisory agencies in the event that people turn to the agency for issues that by nature are private disputes between private persons and should be resolved in civil court.

In public administration, the characteristic of horizontal topics is that in terms of content, a number of other institutions are associated with them, to a greater or smaller extent. I will give you a few examples of connections to the topics of personal data and public sector information:

1) Information System Authority: cybersecurity, supervision of databases, support systems for state information system, managing the information gateway for public sector and organising open data;

2) Police and Border Guard Board: investigating offences associated with personal data, web constables, internal control for preventing departmental misuse of police databases;

3) Health Board: supervision of the provision of health care services, particularly its obligation to maintain records;

4) e-Health Foundation: information security and supervision of the use of e-health information system;

5) IT-support institutions servicing areas related to the government of ministries: organising information security;

6) Among IT-support institutions, the Information Technology Foundation for Education is also the leader of promoting digital awareness;

7) Ministry of Internal Affairs: information security and the supervision of the use of the population register;

8) Last year, the Ministry of Foreign Affairs included data protection in the regular supervision of consular posts.

Several other areas of supervision also include components of protection of data and private life, including:

1) Consumer Protection Board: consumer protection and supervision of advertising;

2) Labour Inspectorate: supervision of Employment Contracts Act;

3) Financial Supervision Authority: supervision of banking and insurance;

4) Technical Surveillance Authority: supervision of electronic communications.

We are closely associated with the Chancellor of Justice. The objective of the Inspectorate is to protect fundamental rights associated with information. The activities of the Chancellor of Justice include all fundamental rights; and this year, supervision of secret surveillance was added to it.

The Director General of the Estonian Data Protection Inspectorate has the right to report directly to the Chancellor of Justice. This enables incorporating the protection of the information rights into the general protection of fundamental rights to a higher degree. It also presents the opportunity to request the Chancellor of Justice to consider initiation of a contitutional court case, if necessary.

IV. Important moments in 2014

a) The priority for drafting guidelines and consulting regarding e-commerce

It is customary for the Inspectorate to prioritise one specific topic for focusing its attention and resources. Last year, this priority was e-commerce. According to surveys, the indicators of our e-commerce are not prominent in international comparison – contrasting with e-banking, for example. The buyer and seller are unable to see each other in an online store, which is why one prerequisite for e-commerce is the customers' trust. Secure processing of customer information that honours privacy helps to create trust.

E-commerce is an important segment for entrepreneurs just starting out – it does not require large starting capital. It is important to small businesses to receive convenient and helpful cross-agency information presented in a simple language.

At the start of the year, we organised a round table on this topic for business organisations, together with the Consumer Protection Board and the Ministry of Economic Affairs. We received feedback regarding which assistance is required from us in real life. As a result, we drafted two guidelines:

- *Information Security and Personal Data in a Small Company*
- *Secure Online Store*

We included practical infotechnological and legal guidelines in these. Hopefully, these will be particularly useful for persons starting out with business. In terms of information security, we also received helpful advice from the Information System Authority.

With respect to both guidelines, we made sure that they could be used for subsequent business consulting upon preparing broader training materials.

We introduced the guidelines at training sessions organised by the Consumer Protection Board and the Association of Estonian e-Commerce.

We prepared two practical guidelines for regular users of information and communication technology equipment:

- *Personal Mobile Devices in the Working Environment* – to supplement the general guideline for processing personal data in employment relationships
- *Deleting Personal Data in Devices* – as a result of monitoring 11 companies operating in the utilisation of electronic equipment

With respect to public sector information, the core topic was, of course, open data or, to put it more accurately, enabling the downloading of machine-readable public sector information. We have consolidated the questions of this topic in the new chapter of the general guideline for public sector information. We also assisted the Ministry of Economic Affairs and Communications with preparing a Green Paper on open data by including a chapter on the protection of personal data and private life.

b) Statistics: the volume of reactive actions decreased

The last year's statistics were surprising. In 2007, the Inspectorate was included into the administrative field of the Ministry of Justice. Within five years (from 2007 to 2013), the volumes of the Inspectorate's reactive actions increased fivefold.
- the number of complaints increased from 110 to 550 (exactly a fivefold growth);
- the number of requests for explanation increased from 251 to 1370 (growth 5.5 times);
- additionally, 1344 calls to the information hotline were answered in the year 2013. We set up the information hotline in 2009, and it has decreased the number of requests for explanation and probably also the number of complaints.

We expected the growth to continue in the previous year, as well. But 2014 was the first year in the history of the Inspectorate when the numbers of reactive actions decreased instead of increasing. This was the case with all complaints and challenges, requests for explanation, consultations, calls to the information hotline and misdemeanour issues.

I could not pinpoint only one reason for the decrease. It is possible that it is at least partly down to the long-term impact of the Inspectorate's preventive work, and drafting of guidelines.

The 30 % growth of the number of registration applications for processing sensitive personal data (from 602 to 902) can be explained by the fact that a large group of data processors completed their 5-year registration period. The decrease in the number of precepts associated with the obligation to register (from 130 in 2012 to 45 last year) can be explained by the Inspectorate's preventive awareness raising activities.

MAIN WORKFLOWS	**2012**	**2013**	**2014**
Explanation and awareness raising activities			
Requests for explanation, memoranda, requests for information	817	1,370	1,144
Calls to information hotline	1,160	1,344	1,141
Consultations	56	69	34
Training (*organised or attended as a lecturer*)	18	19	24
Supervision activities			
Comparative monitoring (*completed*)	4	4	6
Complaints, challenges, misdemeanour notices (*submitted*)	404	550	413
Self-initiated supervision cases (*initiated*)	191	171	152
Precepts in supervision cases	187	121	86
incl. precepts related to registration obligation	*130*	*68*	*45*
On-site inspections visits in supervision cases	23	15	48
Misdemeanour cases (*concluded*)	43	29	11
Fines (*in misdemeanour and in supervision cases*)	39	22	8
Permit and special proceedings			
Applications related to the processing of sensitive personal data or to data protection officers	608	602	902

Approval applications for databases (*by way of the administration system for state information system*)	84	89	115
Permit applications for scientific research without the consent of data subjects	13	17	13
Permit applications to data transfer to third countries	7	6	13
Requests from data subjects regarding cross-border information systems in Schengen, Europol, etc.	4	6	6
Development of legal practices, policy advice			
Guidelines	4	12	6
Opinions on draft legislations (*outside of approving databases*)	21	30	28

c) We increased the volume of self-initiated supervision activities
To compensate for the decrease in the volume of reactive actions, we have increased the volume of self-initiated preventive activities.

The most voluminous supervision project is the annual traffic light monitoring of websites and document registers of institutions. The name is derived from our practice of giving overall assessments to the monitored objects in traffic light colours. The year before last we monitored governmental authorities (43), last year all local governments (215) and this year both local governments and county governments (15).

The traffic light monitoring of local governments in 2014 was followed by a competition for the most transparent local governments. In the course of this, we also assessed the transparency of council activities (reflecting the activities on the website) in addition to assessing legal requirements. The competition winner in the round for larger municipalities was Põlva; and in the round for smaller ones, Torma rural municipality.

In addition to monitoring local governments, we carried out three other surveillances last year:
- surveillance of quick loan companies (19) together with the Consumer Protection Board;
- surveillance of free applications for smart devices (30) based on the methodology harmonised in the course of the global internet sweep campaign;
- surveillance of companies engaged in the utilisation of electronic devices (11), based on which we drafted the guideline *Deleting Personal Data in Smart Devices*.

We also completed the previously started:
- special surveillance of document registers of institutions (144 institutions);
- monitoring of legal bases for restrictions on access to public sector information (retaining 86 of the 177 restrictions previously used). The Ministry of Economic Affairs and Communications can use the surveillance results as classification upon developing document management for the public sector.

Comparing the last year and the year before the last, we also increased the number of on-site inspections (from 15 to 48). We conducted five data protection audits.

The audit on medical spas (sanatoriums) was carried out as a joint activity (based on a joint questionnaire) of Baltic data protection inspectorates. In Estonia, the protection of personal data was audited in 12 spas.

Last year, we paid close attention to health care and welfare services. In addition to auditing spas, we organised:
a) data protection audits in the Lääne County Hospital and Tallinn Children's Hospital;

b) with respect to adhering to the requirements of registering the processing of sensitive personal data, we organised unannounced inspections to ten pharmacies;
c) with respect to the data quality in health care, we received source data (issues with document-based determination of disability according to the e-health information system) from the Social Insurance Board and participated in unannounced inspections carried out by the Health Board to three health care service providers. We corresponded with other problematic health care service providers;
d) we also inspected the requirements of secure forwarding and processing of sensitive personal data in the course of unannounced inspections to ten care homes.

At the Tax and Customs Board, we inspected the compliance of automatic decisions made with respect to self-employed tax payers with the Personal Data Protection Act.

Last year's activities are commented in detail in the following chapters.

V. Important moments in 2015

a) Health care and welfare: the priority is a guideline for the flow of information regarding persons in need
Our priority for this year is the preparation of a guideline with respect to people requiring medical and welfare assistance regarding matters related to the flow of information. Such information is held by, for example, kindergartens, schools, family physicians, hospitals, the police, etc.

This information may not arrive where necessary – particularly to the local government as a welfare, child protection and guardianship authority. Registers developed based on the submission of applications are also incomplete – no information is generated without applications.

Information regarding the need for medical and welfare assistance is naturally sensitive and must be carefully kept. However, this information often tends to get stuck and fails to move forwards. Data protection that hinders matters is also given as an excuse.

We will map relevant standard situations and issues, meet with relevant authorities and organisations and prepare an explanatory guideline.

Secondly, we will prepare a legal analysis for cross-border flow of medical information (incl. cooperation with respect to legal protection).

We will also inspect 20 family physician practices on site. The control plan has been prepared with consideration to the information security requests of the Information System Authority.

We will carry out an on-site inspection of an emergency medical care provider (data flow between the emergency medical staff, hospital, e-health and the emergency centre), and a data protection audit in one major hospital.

b) Data management in the public sector
In addition to health care and welfare, the second larger field of activity this year is the information security and data quality of data management in the public sector:

We will prepare an information protection guideline for authorities. The official system of security measures (three-level IT baseline security system ISKE) is only applicable to databases; everything else is guided solely by the provision in the public sector information Act that provides that information deemed for restricted use shall be protected (subsection 43 (1)).

We will carry out surveillance in several IT support institutions, the Tax and Customs Board (management of access rights, retention deadlines, cross-border data exchange), the Rescue Board (rescue information system), Statistics Estonia (principle of minimalism upon collecting personal data).

We will also inspect the use of surveillance equipment in law enforcement and lawful disclosure of personal data in the court system and the criminal records register.

Implementing ISKE and carrying out data security audits in databases has come under our scrutiny. Among others, we will inspect the 40 most important databases for carrying out the register-based census in 2020.

We will inspect data protection in the document registers of 50 educational institutions. We have recently completed the supervision of the three most common study information systems used in schools.

c) Personal data in customer and employment relationships
We will inspect the management of personal data of job applicants, employees and former employees in the four largest retail chains. We have selected these companies due to their large personnel turnover. Latvian and Lithuanian Data Protection inspectorates have agreed to cover this project as a topic of the annual Baltic joint supervision. Surveillance will therefore take place pursuant to a joint survey in all three countries.
We will also carry out supervision in:
- three companies selling used online equipment (that they would not publicly disclose the personal data of previous users – we have provided relevant suggestions in the guideline *Deleting Personal Data in Devices* prepared last year based on comparative monitoring);
- five communications undertakings (security of client information);
- three online stores (giving appropriate information to the customers – we have provided relevant suggestions in the guideline *Secure Online Store* prepared last year based on comparative monitoring).

In the course of comparative monitoring of debt collection companies, we will inspect their data sources and retention deadlines.

We will also monitor companies using telematics (particularly the electronic monitoring of company cars). Monitoring results will probably enable us to revise the practical instruction material.

We are also planning to prepare information material regarding the privacy of portable smart devices (watches, bracelets, etc.). We are particularly interested in the use of medical information.

With respect to using drones (unmanned flying devices equipped with recording and surveillance equipment), we will revise the Inspectorate's 2013 guidelines for the use of cameras. The relevant chapter is currently awaiting approval from the Civil Aviation Administration – in the interests of the reader, we hope to include recommendations from both authorities (both in terms of personal data protection and aviation safety) in one guideline.

We also need to amend the guidelines on cameras with explanations regarding the preliminary decision of the European Court of Justice on 11 December, 2014, on security cameras.

We will carry out supervision in ten companies with respect to using electronic contact information for direct marketing. We will also inspect the standard terms of insurance companies in the event of direct marketing.

d) Availability of public sector information
We will carry out traffic light monitoring of websites and document registers of local governments and county governments by giving general assessments in traffic light colours. We will award the title of the most transparent local government based on additional criteria. We have discussed the monitoring survey with umbrella organisations of local governments.

We will also carry out surveillance in order to assess how institutions perform the requirements of legislations and the recommendations of the general guideline for public sector information and the Green Paper on open data with respect to downloading machine-readable public sector information.

We will revise the general guideline for public sector information with two new chapters, which address the publicity of using Structural Funds of the European Union and public procurements.

e) International cooperation

The central topic for international cooperation regarding data protection continues to be the reform agenda for the Data Protection Law of the European Union proposed in January 2012. On 23 January, 2015, we hosted an expert forum for discussing the impact of the reform with the help of the Office of the Chancellor of Justice.

The Estonian Data Protection Inspectorate contributes to the topic of practical cross-border cooperation as part of the task force of European data protection institutions.

The cooperation of Estonian, Latvian and Lithuanian Data Protection Inspectorates has been consistent. Each year, we have carried out supervision using a joint survey in order to ensure uniform level of data protection in the economics of all three Baltic countries.

VI. Recommendations for public institutions

a) Information security in the public sector requires stronger control

Outwardly, everything seems to be in order with the information security in the public sector:
- the legislations require institutions to protect personal data and other information subject to restrictions on access (subsections 7 (3) and (4) of the Administrative Procedure Act, sections 24-26 of the Personal Data Protection Act, section 43 of the public sector information Act);
- the government requires the government authorities to apply harmonised measures of information security pursuant to its regulation (*System for Managing Information Security*);
- thorough security system applies to public sector databases pursuant to a regulation of the government (three-level IT baseline security system ISKE);
- new databases are coordinated in the administrative system for the state information system, in the course of which potential deficiencies can be sifted out;
- information security supervision is conducted by two institutions:
    the Information System Authority watches over both database maintenance and the electronic security of all vital services, and it performs generic tasks of a cybersecurity institution;
    the Estonian Data Protection Inspectorate watches over both the protection of personal data and the availability of public sector information, whereas the latter also includes supervision of the application of restrictions on access.

The Inspectorate finds that in practice, everything is not as it seems. A simple example: a large number of institutions have ignored the obligation to commission a regular data protection audit upon maintaining databases. Required notes are not entered in the administration system for the state information system, which makes it more difficult to get an overview.

In the event of large and complex systems, without an impartial external assessment, the management board of the institution cannot ensure that information security and data protection risks, particularly the institution's own personnel risk, are hedged.

I would like to remind the management boards of all institutions that in this digital age, poor information security is just as dangerous as a badly protected state border, broken door lock or unattended wallet. The manager is liable for ensuring information security as much as for, say, organising the accounting.

I expect the Information Security Authority to effectively contribute to and cooperate in:
- matters associated with meeting the coordination requirement for databases;

- matters associated with the accuracy and integrity of data entered in the administration system of the state information system with respect to databases;
- matters associated with implementing supervision on ISKE and the system for managing information security in government authorities, including the performance of the obligation to audit databases.

Supervision itself is not enough – uncoordinated and unaudited databases must not just be left without investments granted from the Structural Funds of the European Union, but they should also be systematically removed from the service of the Data Exchange Layer of databases (X-Road) as sources of risk.

The regulation on coordinating databases has deviated too far from the reality and requires immediate revision. In practice, the number of object types to be coordinated has become significantly larger than the regulation provides for. Even the circle of institutions granting coordination is wider than the regulation provides for. The Inspectorate has submitted its recommendations to the Ministry of Economic Affairs and Communications in its letter no. 1.2.-2/13/2001 of 18 November, 2013.

I will make the organisation of information security in the public sector my personal priority and plan to demonstrate consistent strictness in the matter. As of this year, the Inspectorate has taken both the application of ISKE and the performance of the obligation to audit databases under scrutiny. We will also prepare a guideline for the protection of information with restriction on access (ISKE is only applicable to databases); the project is currently awaiting the Information System Authority's opinion.

b) Making public sector information available as open data

As of 1 January, 2015, all public sector databases must be downloadable through the Estonian information gateway in a machine-readable format according to the subsections 29 (3) an (4) and section 58.2 of the public sector information Act).

I find the implementation of these provisions of law to be unsatisfactory, because as at this moment, only 23 databases have been made available for machine-readable use directly in the respective data repository by way of the information gateway.

It is not easy to criticise the institutions maintaining databases, however, because:
- the information material necessary for carrying out machine-readable disclosure is a relatively complicated change – the final version of the Green Paper on machine-readable disclosure of public sector information – was not completed before the provisions of law were passed but instead, two years later, and only a month before the deadline for full implementation thereof;
- repository for open data was opened for database custodians for disclosing their datasets only after the full entry into force of the provisions of law on open data, i.e. in January 2015.

Fortunately, the situation is not quite as bad substantively. Databases that are the most important for users – for example, court registers, databases of the Land Board and the Estonian Road Administration – were ready for machine-readable use much earlier, partly even as of the last few years of the previous century.

The greatest risk to the privacy of people may arise from databases containing personal data that are maintained by institutions that have not been exposed to the topic of open data before.

I once again strongly urge all institutions maintaining databases to carry out an inventory regarding the ability to download machine-readable data and assessment of impacts. This helps to:
- assess the importance of your information assets as open data;
- review the technical side of ensuring machine-readability;
- map the severity of interference with privacy and make any necessary changes. The ability to fully download the entire database together with the option to combine the received information with datasets

from other sources creates a significantly greater opportunity for profiling people than individual inquiries and request for information gave cause to believe.

As such, I ask the managers of all institutions to keep the following in mind: with respect to the public section of an institution's document register, the dataset included in correspondence with private persons must be made impersonal (using initials) before enabling machine-readability.

c) Broader implementation of an official e-mail

I have drawn attention to the unsatisfactory quality of contact information collected in institutions and databases for people in my annual reports for 2008, 2011 and 2013 alike.

The public sector should use the data provided in the population register in their communication with people. Data updates received upon communication with any public institution should also arrive in the public register. Institutions should not collect duplicate contact information.

Unfortunately it is clear that these principles have still not come into force, among others due to the incompatibility between the Population Register Act and procedural laws. In administrative and court proceedings, contact information for natural and legal persons is collected predominantly separately, often going so far as to collect information separately for each case. The result is poor data quality (contact information is a quickly changing type of information) and continuous procedural delays upon delivering documents.

At the same time, the state has created an official e-mail address for all natural and legal persons (....@eesti.ee) and, once logged in, personalised access both to the central information gateway (www.eesti.ee) and departmental portals.

As I was introducing last year's annual report, I recommended making the official e-mail and electronic delivery a preferred communication channel between the institutions and people. This would allow us to overcome the poor quality of contact information for people available to the public sector. This would also make public administration quicker and cheaper.

Relevant offices were supportive of the suggestion. To implement the suggestion, I called a task force comprising the Ministry of Justice, Ministry of Economic Affairs and Communications, Ministry of Internal Affairs and Information Systems Authority.

The task force discussed what could be done first without amending the laws:
- use the official e-mail address personal identification code@eesti.ee or registry code@eesti.ee to send notices to people;
- the notice for delivering a procedural document contains a respective link;
- in order to open the link, the person must identify themselves by logging in to the respective website (the 'My inbox' service to be created in the Estonian information gateway www.eesti.ee, e-Tax Office, e-File or other portal);
- the Administrative Procedure Act requires the person's consent for electronic delivery, but it does not exclude the option of giving a general advance consent. We have therefore drafted a general consent text that conforms to the law but is written using simple language (separately for a natural and legal person);
- the consent is suitable both for people that have not yet set up their official e-mail address and people that have already done so (current terms of use of www.eesti.ee do not meet the terms of the consent for electronic delivery required by law);
- by opening the linked document (for that, the person has to identify themselves by logging in), the procedural document is deemed delivered, and opening the document leaves a digital trace;
- to ensure that the registry code-based official e-mail address is not misused, it is permitted to be used only for sending procedural documents. The Information Systems Authority technologically filters the circle of senders.

Technological preparation is currently underway in the Information Systems Authority. The fact of giving consent by a specific person must be available to the institutions that send notices or procedural documents to the person. The digital trace left by opening the delivered document, provided that the trace is not left in a respective portal (e.g. e-Tax Office), must make its way through the Estonian information gateway to the administration system of the institution that sent the document. We are also hoping for assistance from the Ministry of Internal Affairs and the Ministry of Justice (recognising the fact of setting up an official e-mail by a natural or legal person either in the population or the commercial register).

In order to prevent the institutions from preferring e-mail addresses disclosed separately in the course of paper correspondence or proceedings, it is necessary that the Ministry of Economic Affairs and Communications makes the respective amendments to the document *Common Bases for Management of Records.* It would also be beneficial to revisit provisions of law concerning the procedural law, as there is excessive preference to paper records particularly in misdemeanour procedure.

We must also reach out to both the public at large (so that the official e-mail addresses would be set up) and the civil servants (so that these would be used as a first option).

In the future, we are hoping for the Ministry of Justice to pass amendments to the law that would make communication with the public sector by way of an official e-mail mandatory to at least the companies.

Because everybody has an official e-mail address, this does not require the people to incur any additional expenses. But it will speed up administrative, court and enforcement proceedings and save money on postal fees. This would also enable us to get an overview of the poor data quality of contact information in the hands of the public sector.

I urge the partner institutions participating in the preparatory work to contribute to the project continuously. I urge all institutions to use the project when it comes into effect. I urge all citizens, residents, e-residents and legal persons to set up their official e-mail addresses in order to make communication with the public sector quicker and more convenient.

d) Introducing uniform web appeals

As an outcome of the joint initiative of the Ministry of Economic Affairs and Communications and the Estonian Data Protection Inspectorate, harmonised forms for web appeals developed by the Inspectorate are currently in the implementation stage. This initiative will hopefully have an impact that spans the entire public sector.

According to the original idea, these forms can be used by anyone wishing to address the Inspectorate in order to submit a request for explanation, memorandum, request for information, submit a complaint or challenge. For this, one has to log into the Estonian information gateway and fill in the respective form.

Data fields that can be filled in automatically or in advance have already been completed. Explanations are given for data fields that require free-form answers.

The Estonian information gateway also enables the applicants to see what happens to their appeal (regarding the reception, revision and response to the administrative information appeal).

The Inspectorate does not need to enter information about receiving the web appeal manually – our document management system automatically takes this data from the Estonian information gateway.

Today, both the websites of institutions and the Estonian information gateway provide hundreds of different document forms for appealing to the institutions. Many of these are inconvenient (i.e. in a PDF-format that needs to be printed out in order to fill in).

Many appeal forms available on the computer network are duplicates. The same requirements apply to a request for information, request for explanation and memorandum, irrespective of whether it is submitted to, for example, rural municipality, city or county government, governmental agency, inspectorate or ministry. The web appeal forms of the Estonian Data Protection Inspectorate can therefore also be used by all the other institutions.

The action plan for 2014-2016 approved by the Government of the Republic for participating in the Open Government Partnership that today comprises 64 countries has a separate clause regarding the preparation of uniform web appeals of the Estonian Data Protection Inspectorate. At this moment, the Inspectorate has handed the prepared materials over to the Ministry of Economic Affairs and Communications.

In the name of a quicker, cheaper and more convenient administration, I recommend the Ministry of Economic Affairs and Communications to take the following steps:
a) make the uniform web appeals mandatory to state authorities once they have been tried out in practice – by making a respective amendment to the *Common Bases for Management of Records*;
b) adopt other forms of appeal – foremost at the level of the local government (for example forms for construction applications) by agreeing on appointing a custodian;
c) in the future, centrally also develop web-based document forms that are sent by the institutions. Their great advantage is an automatic management of restrictions on access and retention. Officers can distinguish parts of the document with free access from those with a restriction already at the stage of preparing the document. Restriction deadlines could be managed by the information system, which would lessen manual work in document management.

VII. Expressions of gratitude

Looking back at the previous year, I have good reason to give my sincere thanks to my colleagues at the Estonian Data Protection Inspectorate, cooperation partners in my home country and abroad, and members of the advisory council of the Inspectorate. It is thanks to you that we can consider the previous year to have been successful both in terms of security of private life, and the availability of public sector information.

I am grateful to the former Chancellor of Justice Indrek Teder – for six and a half years I felt the kind support of the chief legal officer of Estonia.

Yours faithfully,

Viljar Peep