ESTONIAN DATA PROTECTION INSPECTORATE

We take care that privacy is respected in the use of personal data and that activities of the state are transparent

IMPLEMENTATION OF THE PUBLIC INFORMATION ACT AND THE PERSONAL DATA PROTECTION ACT IN 2013, RECOMMENDATIONS FOR 2014

April 2014

CONTENTS

Other parts (chapters 1-5) of this report are available in Estonian language: http://www.aki.ee/et/inspektsioon/aastaettekanded.

EXECUTIVE SUMMARY BY THE DIRECTOR GENERAL

Why the Data Protection Inspectorate?

Inviolability of family and private life and the right to request information collected about oneself are fundamental rights. The Constitution also ensures the right to receive information about the activities of authorities.

We protect the right to privacy and **public information**

Rights pertaining to information are time-critical. The longer the proceedings of a breach are, the harder it becomes to capture the personal data that has leaked into cyberspace. Long proceedings lead to the requested public information losing all value for the inquirer.

Therefore, in order to efficiently ensure information rights, we need a law enforcement authority in possession of sufficient investigation, decision-making and enforcement powers.

At the same time, the Inspectorate should remain independent in its decisions. It is otherwise impossible to provide trustworthy protection with respect to authorities and businesses.

By protecting the right to privacy of individuals and public information, we also serve general interests. Without people's trust, it is difficult for both the public and business sector to create and develop e-services and databases. By observing that personal data is not misused, we create trust and contribute to the development of an information society.

Protection of personal data and access to public information impacts society on a larger scale

However, protection of personal data does not only affect economic development. The authorities collect personal data even if the person does not want it and sometimes has no knowledge of it. This is necessary both to ensure domestic legal order as well cross-border freedom of movement. However, it is in the interest of sustainability of a democratic state based on the rule of law that this information is not collected in excess, its use is controlled and that the data is not stored for too long.

Accessibility of public information is important for the individual in need of specific information. But it also affects the whole society helping to ensure more efficient control over exercise of public authority, use of public money and performance of public duties.

The Inspectorate shall interfere in case of breach of information rights based on complaints as well as on its own initiative. The rapid development of society and information technology requires us to also function as an authority of analysis, prevention and awareness raising.

A look at five years ago and forward

Last year, on October 1 my 5-year term in office as the director general of the Inspectorate ended and I was appointed to the same position for the next five years. I highly value Riigikogu Constitutional Committee's unanimous support for my reappointment.

As it is the end of one term in office and the beginning of another, it is reasonable to make a short review of the past and look towards the future – what the Inspectorate looked like 5 years ago compared to today and how we want to see ourselves in 5 years from now.

When brought under the administration of the Ministry of Justice in 2007, the Inspectorate's structure consisted of the Director General, Deputy Director General, 3 departments and 3 services. In total, 21.5 out of 31 permanent positions were staffed, 8 of them directors. In 2007, 5 officials resigned and 7 more left during the following year primarily due to low salaries.

Inspectorate in 2007:

officials 21.5, reviewed 110 complaints, 251 requests for explanation

My predecessor wrote in the foreword of the 2007 report that the Inspectorate has changed from a registration agency of personal data processors to a supervisory authority. The earlier focus on the registration procedure required a lot of resources but had little impact. Instead, supervisory activities were expanded: employees from one service went on on-site verification visits, while others processed documents. There was no specialization according to different areas.

In 2007, the Inspectorate reviewed 110 complaints and challenges. Last year, this number was 550 – a 5-fold increase.

Inspectorate in 2013:

officials 18, reviewed 550 complaints, 1370 requests for explanation + 1344 helpline calls

The number of requests for explanation and memoranda increased from 251 (2007) to 1370 (2013) i.e. 5.5 times. This would have been higher but we launched a helpline in the meanwhile. This allows to answer simpler questions quickly over the phone – last year we responded to 1344 calls.

As of 2013, the Inspectorate's structural units are 2 departments. All 18 positions of officials are ensured with a salary fund, no vacancies are kept. There are no contract employees – nobody in the Inspectorate deals with support services only.

The quantitative and qualitative strengthening of supervision has, among other things, been supported by:

1) replacement of functional specialization (on-site verification visits or document-based work) with sectoral specialization (healthcare, police work, the media, financial sector etc.) – an inspection official must be familiar with the inspected field,
2) we prefer supervision proceedings, which eliminate problems, to misdemeanour proceedings based on penalties,
3) in simpler cases, we implement simplified supervision proceedings,

4) the web-based registration process by personal data processors enabled to bring additional staff into supervision,
5) we perform regular internal quality assessment.

Reacting by supervision and misdemeanour proceedings means dealing with individual cases. However, figuratively speaking, in addition to dealing with the trees, we want to deal with the forest. We have introduced new self-initiated supervisory forms – monitoring and auditing. Monitoring covers many objects in some important inquiry. Audits are aimed at checking a big and/or sensitive organisation to prevent problems.

We try to use the resources left after reacting to problems in a supervisory manner as efficiently as possible. Instead of 1 information security expert, the Inspectorate includes an IT specialist and 2 security experts without increasing the number of staff. Awareness raising is the task of 3 advisers (Public Relations Adviser, IT specialist, General Unit Adviser). The Legal Adviser (Chief Legal Officer) deals with legal analysis and quality assurance.

In order for the authority not to focus too much on the responsive proceedings conveyor, each year we make a detailed plan of self-initiated activities in supervision, prevention, giving information as well as analysis.

Information rights and the Inspectorate in 2018

What will the Inspectorate and the field of information rights look like in 5 years?

Our main task is the protection of individuals from authorities, and also the protection of an individual's rights from companies. However, the fastest-growing workflows are the ones that require the protection of one individual against another individual. This trend will probably only worsen – this covers social media, ever more common recording and surveillance technology (including drones) as well as face recognition software to name just a few. The amount of information about individuals keeps increasing in the global cyberspace.

Undue interference by supervisory authorities in private disputes should hopefully be restricted by § 4 (2) of the Law Enforcement Act entering into force on 1 July, 2014. In this context, I predict that unless new extensive tasks are imposed on the Inspectorate, in 5 years we will probably remain at our current size. I believe that the automation of document circulation and web-based supervision should help manage the increase of work.

In order to improve prevention and awareness raising activities, the number of networks the Inspectorate is either managing or participating in will increase.

Growth can also be predicted in the share of international work. Firstly, workload will probably increase in the working party of European data protection authorities regardless of whether and in what way the data protection rights reform initiated by the European Commission in 2012 is realized. Secondly, there will be an increase in practical cross-border cooperation in areas of prevention and supervision. Cooperation between data protection inspectorates between Estonia, Latvia and Lithuania has been successful. We also need joint cross-border activities with other countries with whom our economy is more connected.

Hopefully, Estonia will contribute, together with other like-minded member states, to improving cross-border cooperation related to data protection, but at the same time inhibit overregulation, unnecessary increase in administrative burden and risks to open society. Internationally, the Inspectorate will contribute to improving practical cooperation.

The development of information society and technology will probably bring a lot of new challenges in the coming years. Reusing public information as open data has not really gained a lot of ground in Estonia yet. The requirement to disclose information in a machine-readable form and as a full downloadable database has firstly not been sufficiently implemented and secondly has not found sufficient use in the private sector.

Most laws about the maintenance and availability of databases date back to the time of transitioning from paper to digital formats when the only option was to make individual enquiries. It can be seen that this subject requires legislative and administrative revision. Considering the extent of diversity of public sector databases, an *ad hoc* response will probably be predominant in the next few years.

Summary of last year's work

Need for creating guidelines

The development of information and communications technology and the information society is rapid. Thus, there is an extensive "grey" area in the acquis of personal data protection and public information. Undefined legal concepts (e.g. excessive damage, public interest) therefore require constant interpretation. Considering how small the Estonian law and language space is, our specialized legal scientific commentary and judicial practice takes more time to develop than in bigger countries.

Therefore, the Inspectorate must focus more on creating guidelines, developing legal practices, in order to ensure legal clarity and legal certainty essential in public administration and business.

Each year, the Inspectorate has undertaken some significant "gray" area subject, organized monitoring, investigations and discussion involving relevant parties and eventually taken the professional idea and practical problems as a guideline.

Camera guide

Last year, this central topic was the use of monitoring and recording equipment. We tried to approach this in a complex manner: use of cameras for private purposes, recording in a public place and at a public event, security cameras, recording to ensure contract enforcement and for journalistic purposes, cameras in children's, educational and public institutions etc. One of the issues causing debate, for example, was whether the kindergarten and school are public places from the point of view of recording and photographing (where consent is not necessary) and if they are, to what extent.

The Inspectorate's Legal Adviser Maris Juha initiated the preparation of "Camera use guidelines", which was our first guideline to be published in the draft legislation information system.

Protection of employees' privacy

In addition to preparing new guidelines, we also try to keep "alive" our other important guidelines – refer to them in our daily work and monitor the need for change. It turned out that in addition to the guideline about personal data processing in employment relations, which was prepared in 2011, a need arose to more thoroughly cover the privacy of employees' use of computers and smart devices.

While in personal relations it is covered by an individual's confidentiality of messages and a communications company's data protection and secrecy obligation, the use of the same devices in employment relations creates a legal triangle – an employee is not the customer of a communications company. The guideline "Employee computer use privacy" initiated by the Inspectorate's IT-adviser Urmo Parm binds together both information technological and legal explanations.

In addition to publishing the answers to questions that are of most interest to employees and employers in our website's frequently asked questions section, we will also publish them in the working life portal managed by the Labour Inspectorate.

Financial sector

Last year, there were several issues in the area of insurance – use of third-party data, storage of personal data processing consents, customer data movement with a broker changing employers. On the initiative of Leading Inspector Merit Valgjärv, we also carried out monitoring of leasing companies in connection with transmission of personal data to insurance companies.

In banking, we performed contract-based and consent-based examination of the processing of personal data and also organized monitoring to get an overview of the practices. The main problems occurred in connection with direct marketing consents. The banks have now adjusted their practices in this area.

Based on problems revealed in practice, we made extensive improvements in the payment defaults publication guideline.

Explanation and awareness raising activities

Formation of the Inspectorate's IT-group has significantly improved explanation and awareness raising activities in the area of information and communications technology. We will publish practical explanations and instructions in the press and on the web. Nine practical recommendations for the safe use of a smart phone by IT-adviser Urmo Parm gathered more than 21 thousand views on the Inspectorate's Facebook wall. Instructions for Facebook applications were viewed more than 10 thousand times, for the setup of browser vendors of a child's computer (directed towards parents) almost 10 thousand times and for deleting ID card user history on a computer 4 thousand times.

In order to help companies to whom reliability of privacy and information security is more important than average, we prepared an information assets balance sheet based on the Finnish example. This can be used in businesses within the framework of the usual annual reporting process to carry out a self-assessment in the area of personal data protection and information security and if desired, to also publish it to gain more trust from customers and partners. The information assets balance will require further promotion for general use.

We also performed awareness raising activities through various forms of cooperation – in the project *Targalt Internetis* (Be Smart Online), with the Association of History and Social Studies Teachers and web constables. On the initiative of Adviser Silver Sarapuu, we prepared comic books related to the protection of privacy to be used as auxiliary materials by teachers at schools.

Conference in cooperation with the University of Tartu Centre for Ethics

In cooperation with Tartu University, we organized the conference "Ethical Dimensions of Data Protection and Privacy. Global and Local Challenges" on 9-10 January, 2013. The selection of speakers was impressive – several top scientists from Estonia and internationally renowned foreign lecturers, including Prof. Beate Rössler and European Data Protection Supervisor Peter Hustinx. The patron of the conference was the President of the Republic, who also held the first presentation on the topic.

For such a high-level and at the same time comprehensive research event, we must first and foremost thank the head of the University of Tartu Centre for Ethics Prof. Margit Sutrop and her team. The conference audience mainly came from a legal or information technological background and I believe both were impressed by the conceptualization of their daily work through ethical values.

Prevention activities in availability of public information

In order to ensure the availability of public information, we carried out another monitoring of state authorities based on web pages and document registries led by Chief Inspector Elve Adamson and published the traffic-light colour-coded results. The Inspectorate's Advisory Council selected the most transparent authority among the five finalists – the National Audit Office won overwhelmingly. For several years, the Inspectorate operates a network of chief information and privacy officers of state agencies in order to solve practical problems.

Coordination of Tallinn ticket sales database

Approval of databases in the state's information system management system is a procedure between agencies, which is dry and dull on the outside and in which the public is not particularly interested. An exception turned out to be the approval of the public transport ticket sales information system in Tallinn.

Since the local government ignored legal and information security-related remarks by the Inspectorate and the State Information System Authority and made use of an uncoordinated database, we initiated separate supervision proceedings, in which we involved experts from both the stated Authority and the Centre of Registers and Information Systems. As a result, personalized data storage periods were shortened, security was strengthened and relevant local government legislation was amended, and the database was subjected to concertation proceedings.

All the changes made as a result of supervision would have come out in due course during the approval of the database establishment plan stage or the approval of implementation stage at the latest.

We believe this is a lesson for all state and local government agencies – solving data protection problems in databases retrospectively is more expensive and cumbersome than screening them out in the course of approval.

We compiled "Database guidelines" to solve practical issues related to the regulation and management of databases.

International cooperation

In cross-border activities, we continued the cooperation between data protection inspectorates of the Baltic countries and supervision carried out using a common methodology on agreed topics.

We completed the tripartite monitoring of the hotels using the trademark *Radisson Blue Hotel*. In monitoring casinos, we discovered a loophole in Estonian legislation regarding the maximum period for storage of video recordings and customer information for the correction of which we gave a

recommendation in cooperation with law enforcement authorities and the union of organizers of gambling.

Data protection agencies in the Global Privacy Enforcement Network (GPEN) carried out the Internet Sweep Day monitoring in May 2013. Within that framework, we examined the existence and comprehensibility of privacy policy in 40 largest retail companies in Estonia.

According to the Directive, the purpose of the activity of the European data protection authorities' working party formed on the basis of article 29 of Directive 95/46/EC is to improve the harmonized implementation of the Directive. To date, the working party's most voluminous activity has overwhelmingly been the preparation of opinions (guidelines), in which we have achieved a considerable proficiency. Policy advice is also dealt with – recently especially with the EU data protection rights reform and in coordinating the solving of cases that have attracted international attention and if necessary, some member authority is given the right to act on behalf of the entire working party.

In October 2013, the Inspectorate presented an initiative at the working party's plenary session to regularly enter on the agenda some organization of practical cooperation – exchange of managerial experiences and agreement on smoother cross-border cooperation procedures. The initiative was supported and was joined by colleagues from the United Kingdom. In all subsequent plenary sessions, all jointly prepared agenda items have been discussed.

Main workflows in numbers

There has been a noticeable increase in the number of inquiries sent to the Inspectorate – in requests for information-memoranda, helpline calls as well as complaints-challenges. This is also shown by the comparison of indicators from the previous year and the year before that:

	2012	2013
Explanation and awareness raising activities		
1. Requests for explanation and memoranda	**877**	**1370**
2. Helpline calls	**1160**	**1344**
3. Training (hosted or attended as an educator)	**18**	**19**
Supervision activities		
4. Complaints and challenges (received)	**404**	**550**
5. Proposals and recommendations (made in the course of supervision)	**196**	**287**
5.a) including during self-initiated supervision	*105*	*108*
6. Precepts (made in the course of supervision)	**187**	**121**
1.6.a) including standard precepts related to notification obligation	*130*	*68*
7. On-site verification visits (made in the course of supervision)	**23**	**15**
8. Comparative monitoring (a specific aspect of many objects are monitored simultaneously)	**4**	**4**
9. Audits (comprehensive data protection assessment of an institution/company)	**7**	**5**
Punishment and administrative coercion		
10. Misdemeanour proceedings (completed), including	**43**	**29**
10.a) related to misuse of the population register	*34*	*5*
10.b) related to misuse of the police database	*4*	*8*
10.c) related to misuse of the health data	*2*	*6*
11. Misdemeanour and coercive fines	**39**	**22**
Permits, approvals and special proceedings		
12. Registration of sensitive data processing (number of requests, including requests related to data protection officers)	**608**	**602**
13. Approvals of public sector databases	**84**	**89**
14. Requests from data subjects regarding their own data in the Schengen, Europol and other international information systems	**4**	**6**
Development of legal practices, policy advice		
15. Guidelines	**4**	**12**
16. More thorough advisory services to institutions and companies (at least 1 meeting)	**56**	**69**
17. Opinions on draft legislation (without the opinions expressed in the course of approval of databases regarding the statutes of databases, see line13)	**21**	**30**

Supervision and punishment policy

In responding to breaches, the Inspectorate's priority is still the quickest possible termination of the breach as opposed to punishment.

This approach is also supported by the study „Access to data protection remedies in EU member states" published by the European Union Agency for Fundamental Rights in January 2014 – data subjects, whose rights have been violated, are primarily interested in the quick termination of the violation.

According to the Inspectorate, disputes related to the availability of public information serve the same purpose – persons making requests are interested in quick and easy proceedings to gain access to information.

For comparison – in supervision cases related to protection of personal data and public information, 287 proposals-recommendations and only 53 precepts were made.[1] In the majority of cases, the violation ends with receiving a proposal or a recommendation.

The punitive response (misdemeanour proceedings) volume has decreased and it mainly includes misuse of professional access rights to sensitive records. Since the violation has already taken place, supervision by making proposals-precepts is no longer relevant, which is why the Inspectorate always responds by initiating misdemeanour proceedings in these cases.

The situation with the population registry has significantly improved. We acknowledge years of systematic usage monitoring by the Ministry of the Interior responsible for the registry. It was probably also helpful that the Inspectorate covered this topic in the media.

In the course of the Road Administration's data protection audit, we examined the vulnerability of personal data in the undisclosed part of the traffic register – this includes the contact information based on the population register. By today, the Road Administration has implemented technical measures and internal control to prevent misuse and based on an agreement entered into last year, notifies the Inspectorate of suspected breaches to initiate a misdemeanour case.

[1] Not taking into account the 68 supervision cases with the obligation to register the processing of sensitive personal data. These are simple proceedings, where there are no separate phases of initiating proceedings, making inquiries and proposals – the violation is obvious and a precept is immediately made in standard wording.

About this year's work

The priority of analysis and awareness raising activities this year will be e-commerce and small businesses. The extent of e-commerce in Estonia is below the European average according to a study. At the same time, it is an area of business, where small newcomers find it easy to start (lesser need for initial capital).

To celebrate the day of personal data protection, instead of the traditional conference in January we organized a roundtable for business organizations and relevant state authorities in cooperation with the Consumer Protection Board. The ideas and recommendations we heard there will be used in our future work. In cooperation with the Consumer Protection Board and the Ministry of Economic Affairs and Communications, we will try to improve the availability of know-how and reliability of e-commerce.

We will draw up practical guidelines for e-commerce and small businesses, which teach how to easily manage legal requirements related to personal data and information security needs. These will be accompanied by recommended sample texts needed by businesses in typical cases. We anticipate that our materials can also be used as part of broader training and consultation activities.

We will also participate in the Consumer Protection Board's awareness raising event and in monitoring e-commerce businesses. Cooperation with the Consumer Protection Board is also effective in other areas. We will continue monitoring quick loan companies and the supervision of the more problematic ones, which we started together last year.

This year, we will also monitor businesses engaged in the utilization of electronic devices, as a result of which we plan to prepare guidelines for deleting personal data in devices. We also monitor user conditions of digital television providers with respect to processing personal data. A practical legal-technical guide is being prepared about the personal smart devices used for professional purposes.

Several activities are directed at healthcare and welfare services. Among other things, there is an agreement with the Health Board about joint supervision in the area of e-health data quality using the Social Insurance Board's observations (problems with document based determining of disability). We also plan to start an internet forum about data protection in healthcare primarily intended for medical workers to raise awareness and receive feedback. The leading partner in this is the e-health foundation. We started monitoring spas and sanatoriums providing health services; the same methodology is used by Latvian and Lithuanian data protection inspectorates.

The right to privacy (protection of personal data) and the right to the confidentiality of messages are regulated differently in Estonia and the violation of these rights is also penalised differently. In order to determine the differences between these two fundamental rights, we conducted explanatory analysis. In this regard, we look forward to opinions of the Chancellor of Justice, the Office of the Prosecutor General, the Bar Association and other parties.

We have agreed with the Ministry of Foreign Affairs that they will include the data protection questionnaire in auditing consular posts and exchange information on this topic. In the interests of maintaining proper and safe cross-border European visa information system, we perform harmonised supervision with the Lithuanian data protection inspectorate.

In the area of electronic direct marketing, in addition to document-based proceedings, this year we will also organize self-initiated inspections to personal data processing locations.

In the area of ensuring availability of public information, we participated in the preparation of the Government's Green Paper on the re-use of machine-readable open data led by the Ministry of Economic Affairs and Communications.

We have understood by now that the general guidelines of the Public Information Act require a chapter of recommendations dealing with open data. We also plan to supplement the general guidelines with chapters on the publicity of public procurements and resources from European Union structural funds.

Access to public information may only be restricted by law. In February, we completed access restriction monitoring to public information. In the course of this, we mapped all the restrictions that state authorities use in their real work. In addition to restrictions arising from the Public Information Act, more restrictions are established in specific acts or derived from them. The Inspectorate was informed about the use of 177 restrictions. After communication with the authorities involved, we found that in the final list of legitimate restrictions, there can be 86 restrictions taking into account current legislation, international treaties and directly applicable EU legislation.

In international cooperation, in addition to Baltic joint activities we will continue promoting practical cooperation primarily in the framework of the workgroup of European data protection authorities and Global Privacy Enforcement Network (GPEN).

Policy recommendations for 2014

Recommendations to enterprises

For companies, in whose activities it is important that customers and partners trust them as personal data controllers and processors, we recommend that when creating e-services and information systems, protection of personal data be integrated from the beginning. Doing this in retrospect is more expensive. On our webpage you will find privacy by design principles and data protection and information security self-help questionnaire. In the same place, we will publish personal data and information security guidelines specifically for small businesses and e-commerce, currently being prepared.

Also, ensure that if they which, a person can easily find out whether, why and how their data was collected and used by the company. This is valid for customers, advertising recipients as well as employees. It is particularly important in web-based services and direct marketing. It could be a good practice to publish such explanations (privacy policy) in simple language on a company's website. Availability of information about a company will increase its reliability, but is also a legally guaranteed right, which also applies outside the public sector.

We also advise companies to observe how the public sector will soon be opening databases for re-use in a machine-readable form. Open data leads to new possibilities to create smart and progressive business solutions.

Recommendations to directors of institutions

We advise heads of public sector institutions to start thoughtfully implementing the requirements of public sector information reuse. Before turning over personal information as open data, it is essential to undertake an impact assessment of privacy infringement. You will find more recommendations in the Green Paper on the re-use of machine-readable public information, the preparation of which is led by the Ministry of Economic Affairs and Communications and supported by the Inspectorate. It is worrying that the Green Paper's policy recommendations are not linked to the state budget. This is particularly important in implementing the free availability of databases for information services that were so far funded by service fees (services provided by the Land Board and the court registers).

Applications sent to institutions by individuals form a large-scale document flow, which is automated very little and fragmented across institutions. The Ministry of Economic Affairs and Communications and the Estonian Information System Authority have taken steps to develop uniform solutions based on the Estonian information gateway www.eesti.ee. This would be easier for the applicants (a single access on the web for communicating with the public sector), and would enable institutions to save on manual work and IT costs. This would also be based on safe data transmission unlike e-mail. Among other things, internal structuring of documents would enable automatic management of public information access restrictions. We call on all institutions to use a uniform information gateway-based solution for their digital communication channels. I am glad to assure you that the Inspectorate has started this process.

We advise all institutions to remember that approval of databases in the state information system's management system is intended to be a filter preventing problems. The events surrounding public transport ticket sales information system in Tallinn should be a lesson for all state and local government agencies that ignoring approval and retrospectively altering IT solutions is more cumbersome and expensive. We recommend "Database guidelines" as a practical advice related to the regulation and management of databases.

Recommendations to the Ministry of the Interior and the Ministry of Justice related to the population register and procedural law

The Inspectorate drew attention to the unsatisfactory data quality related to residence and contact information in the population register in its reports in 2008 and 2011. This has a seriously deteriorating effect on the speed, efficiency and cost of the entire public sector administration.

The amendments to the Population Register Act adopted on 16 February 2011 constitute progress, according to which changes in place of residence and means of communication can also be made through the court, the notary, the bailiff or some other institution established by regulation of the Government, with whom the person comes into contact. Progress can also be seen in the clear prohibition that other institutions cannot create duplicated small population registers based on their procedural data. The Inspectorate has also checked the avoidance of duplication in its supervision activities.

Unfortunately, we are still on our way to improving information quality of the population register – procedural laws are not compatible with the logic of the Population Register Act. The list of institutions through which it is possible to further renew population register data is limited (e.g. the Unemployment Insurance Fund and the Health Insurance Fund are not on the list, the Defence Resources Agency does not deal with notices of residence). The bottleneck effect is also caused by checking the correctness of residence data (whether the person is the owner of the place of residence or he/she has the owner's consent). Thirdly, more emphasis should be placed on electronic contact data collection and quality assurance.

In order to improve information quality, the Inspectorate recommends:

1) the procedural laws (administrative, misdemeanour, court procedural law) should as a first choice be based on electronic communication (this is particularly underestimated by the law on misdemeanour procedure),
    - to start using addresses ending with @eesti.ee more broadly by providing their alignment in recurring transactions, where people can communicate with the public sector using the Internet and providing a legal consequence to the alignment,
    - to establish assumption of use for delivering procedural documents of electronic contact data if a person communicates with an institution electronically on their own initiative (this currently requires a separate consent, in case of improper course of procedure, a person can change their mind about consent);
2) include assumption of correctness of population register information in procedural laws and a procedural consequence in case of failure to renew information (similarly to assuming the correctness of commercial register address information in case of legal entities);

3) regarding delivery, to provide legal meaning to the previous other place of residence entered in the population register in addition to the current place of residence (which is published during proceedings and entered in the population register by the institution except in cases when a person legitimately requests that these data remained used only specific proceedings);
4) to expand the circle of institutions, who submit changes in information regarding place of residence, place of stay and means of communications to the population register.

Recommendation to the Health Insurance Fund and the Health Board on e-health

The Estonian e-health information system is a remarkable achievement in terms of its idea and technical execution. Unfortunately, not all parties communicating data are completely fulfilling their obligations, which is why all necessary information does not reach the information system. This contradicts one of the basic requirements of personal data processing – the principle of information quality. The Inspectorate advises the health insurance fund to keep in mind that the prices of healthcare services also include e-health data entry, which must be taken into consideration in making payments. We remind the Health Board that supervision of documentation of healthcare services is a direct responsibility of the Health Board.

Recommendation to the Ministry of Economic Affairs and Communications regarding data housing services

The Electronic Communications Act establishes an obligation to maintain the confidentiality of customer and other personal data and foresees a penalty for the violation of this obligation by telecommunications operators.

At the same time, data housing service providers, who enable the use of e-mail with the same domain name in addition to housing a website, cannot be regarded as telecommunications operators. They operate on the basis of the Information Society Services Act. In the given case, legislation treats the obligations of companies providing similar services and their customers' right to privacy unfoundedly differently.

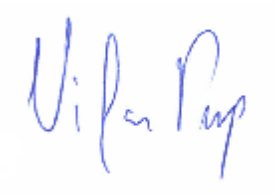
Recommendation to the Ministry of Justice regarding self-employed persons deleted from the register

Sole traders who have terminated their activities complain that contact information entered into the commercial register as contact data is public even after deletion from the commercial register. This means unwanted advertising flow and remaining being recorded in information catalogues and phone books. As a self-employed person is primarily a form of small business, the public contact information of the self-employed person more often than not coincides with their home address and personal means of communication.

Today, the commercial register includes more than 32 thousand sole traders, the number of deleted traders also reaches thousands. The Inspectorate suggests that the contact data files of the self-

employed persons should be closed after the termination of activities (§ 28 (3) of the Commercial Code).

Yours sincerely,



Viljar Peep

Director General of the Data Protection Inspectorate