EXECUTIVE SUMMARY AND POLICY RECOMMENDATIONS FROM DIRECTOR GENERAL

Does data protection hinder security and innovation?

The threat of terrorism is more and more apparent in our homely Europe. In that light, it has often been asked whether the protection of personal data hinders the ensuring of security.

After the Brussels bomb explosions on 22 March, I read a newspaper and found an opinion of a top official of Estonian internal security: "*Europe is largely divided in a dispute between two schools. The choice is whether to protect the people or to protect the data. Fact is, a lot of things are not done or are done insufficiently because we have made data protection into an orthodox dogma.*"

I do not share the view of fundamental opposition between security and data protection. It is understandable that the threat of terrorism must be prevented. It is understandable that extensive data analysis and also covert surveillance have to be used for the prevention. It is understandable that cross-use of databases must be allowed for the prevention.

But do we want a situation where the data analysis and the surveillance data to prevent terrorism and severe crimes can be collected in any manner at all? Or later used for anything and given to anyone? Such information arrays are sensitive, they quickly became obsolete and are frequently based on assumptions, and the results of machine data processing are often not reviewed by a human. Do we want such data to be held forever in data stores? Do we want to see no unbiased control over the collection and use of such data?

The possession of sensitive information is a weapon and it can be used for good and for bad. If we abandon control over it, we will move towards a world not much different from the dreams of many terrorists after all.

Prevention is very important to ensure security. But security and data protection must not be set to oppose each other. We need balancing frameworks and rules when collecting and using personal data for security purposes.

This is why data protection is also a part of the pan-European law enforcement databases. It is so in Schengen and Europol information systems, the visa information system, the Eurodac database of fingerprints, the customs information system, etc. By the way, neither European nor the Member States' data protection law regulates the databases of intelligence institutions and their cross-border use.

I also do not consider it proper to see such opposition in other fields of life, either. Looking at the modern digital economy and e-services, data protection is one of the necessary building blocks for their development.

If people do not trust businesses and institutions with the collection and use of the data pertaining to them, any development of e-services becomes difficult. We are losing a direct contact with the other party; instead, we communicate with their information system. Therefore – the more the society digitalises, the more we need trust concerning data protection.

Thus, we also need rules here – how personal data can be collected, how long the data can be used, when the data can be handed over, when the data collected for one purpose can be used for another purpose, how people themselves can access the data collected about them, etc., etc.
But I agree with the security official referenced above, in that data protection must not become a thing in itself. We need balancing rules and their common-sense implementation, not a full brake on necessary activities.

Data Protection Inspectorate in 2015

I now provide a summary of our last year's activities in numbers, as a comparative table:

OPERATING INDICATORS	2012	**2013**	2014	**2015**	*incl. 2015 IKS, EES // AvTS*
Soft law making, policy advice					
Guidelines	4	**12**	6	**4**	
Opinions on draft legislation	21	**30**	28	**35**	
Communication					
Questions	817	**1,370**	1,144	**1,369**	1,124 // 245
Help line calls	1,160	**1,344**	1,141	**1,136**	915 // 154
Consultation meetings (to enterprises, authorities)	56	**69**	34	**33**	27 // 6
Training courses (organised or lectured at)	18	**19**	24	**18**	
Legal proceedings					
Circulars (without initiating supervision)	-	-	-	**5**	
incl. address of circulars				***149***	
Comparative monitoring	4	**4**	6	**14**	
incl. the number f monitored entities				***412***	
Complaints (filed)	404	**550**	413	**446**	329 // 117
Self-initiated supervisory cases (initiated)	191	**171**	152	**384**	116 // 240
incl. preventive data protection audits	*7*	***6***	*16*	***24***	
Inspections on the spot (in supervisory cases)	23	**15**	48	**35**	
Recommendations (in supervisory cases)				**299**	
Precepts (normally preceded by a recommendation; normally includes a warning about coercive fines)	187	**120**	86	**77**	
incl. in the field of registration (without prior recommendations)	*130*	***67***	*45*	***28***	
Misdemeanour cases (closed)	43	**29**	11	**16**	
Penal law fines (misdemeanour punishment), coercive fines (repeated coercive measure in supervisory cases)	39	**22**	8	**15**	
Special proceedings					
Registration applications (processing sensitive personal data or appointing a responsible person for it)	608	**602**	902	**540**	
Approval requests for databases (upon establishing, taking into use, changing data, terminating)	84	**89**	115	**167**	
Permit applications for scientific research without obtaining the consent of data subjects	13	**17**	13	**29**	
Permit applications for data transfer to 3rd countries	7	**6**	13	**8**	
Applications concerning own data in the databases of Schengen, Europol and other cross-border databases	4	**6**	6	**10**	

About the preparation of guidance texts

The abstract nature of data protection law and the speed of information technology development dictate the need for explanatory helper materials and also require data protection institu-

tions to have transparent opinions. This is why we contribute to the preparation of guidelines covering both legal and information technology matters.
The manual „Isikuandmete avalikustamine meedias: Andmekaitse Inspektsiooni sekkumiskriteeriumid“ [“*Disclosure of personal data in the media: Data Protection Inspectorate’s intervention criteria*”] covers both professional journalism and social media. We reviewed our opinions in light of the Law Enforcement Act. We raised the intervention threshold on media disputes because these are normally private law disputes with no public interest for intervention. Such disputes need to be resolved in court, not through an administrative body.

For example, we usually do not initiate supervision if someone requests that the data about expired punishments be removed from the media. Nothing stops an offender from suing an applicant in court. Cases involving minors are an exception. We also intervene if someone acquitted in court needs help.

There are three manuals that help with issues encountered in practice, where information technology and data protection intertwine:

- „IP-aadress ja privaatsus“ [“IP address and privacy”],
- „Kantavad seadmed ja privaatsus“ [“Portable devices and privacy”],
- „Metaandmed ja privaatsus“ [“Metadata and privacy”].

We have also made amendments to earlier manuals, to keep them up to date.

About legislative consultations

Among draft legislation, 35 drafts were those for which we were individually asked for an opinion or for which we opined on our own initiative. We additionally reviewed 167 database co-ordination applications – this includes the reviewing of draft statutes or some other draft founding documents of the databases.

I acknowledge that many of our comments are repeated from draft to draft. For example, that the purpose of collecting persona data should be worded specifically as possible (otherwise it would be impossible to assess what is necessary to collect and what is not). Or that the statutes should be as specific as possible concerning the contents of the data. Or that the time limits for preserving the data must be set as well, and not randomly at that.

I can highlight three remarkable examples among the legislative disputes of the last year:

a) **The plan to have the Draft Act Amending the Work Ability Allowance Act grant insurance providers direct access to the e-health data.** The amendments were added to the Draft Act after a co-ordination round. We considered this kind of access impermissible. The Social Committee of Riigikogu (Parliament) agreed with us and the Ministry of Social Affairs took back the amendments. With that Draft Act, it was the first time that I used my prerogative to turn to the Chancellor of Justice with an extraordinary rapport. I asked that the Chancellor of Justice consider the initiation of a constitutionality review case if the Draft Act were to be adopted. Fortunately, it was not needed;

b) **The Draft Act Amending the Taxation Act was intended to grant the Tax and Customs Board the right to get communications data from communications undertakings, and access to all databases for the purpose of risk assessment (tax intelligence). It also prescribed the publishing of the persons having received a**

grant from associations subject to income tax incentive. We considered those plans excessive. Concerning the communications data, the preparers of the Draft Act took half a step back and abandoned the asking for details of communications services. We still consider unlimited access to all databases to be excessive. Why are e.g. health data needed for tax intelligence? The wish to publish the names of grantees is incomprehensible. This information is available to the Tax Board, but what added value comes from publishing them in the Internet? I remind you that associations subject to income tax incentives and paying grants include also religious associations, support associations for the disabled, etc. The Draft Act has made its rounds and reached the Ministry of Justice, to which we presented our continuing worries;

c) **The establishment of the database of traffic accidents was planned to grant public access to the anonymous statistics of traffic accidents**. Everyone interested would have been able to learn the data of every victim of every accident: address, gender, age, weight, length, health disorders significant for the accident, the severity level of injuries, vehicle data, the time and place of the accident, even photographs. The preparers of the Draft Act thought that the database was anonymous because it contained no names and personal ID codes of the victims. Naturally, such a database cannot be called anonymous by any stretch. It was incomprehensible what the purpose and gain of such publication was supposed to be.

About communication work

Replying to queries for explanations is one of our most intensive work areas – there were 1,369 of such queries filed last year. Additionally, the Inspectorate's officials take turns on telephone watch – the helpline enables faster answering of simple questions. Last year's 1,136 calls to the information hotline were divided as follows:

- 154 questions about the accessibility of public sector information and access restrictions,
- 147 questions about the publishing of personal data on the Internet (or ceasing the publishing),
- 108 questions about the use of personal data in employment relationships,
- 102 questions about the registration of the processing of delicate personal data,
- 78 questions about the use of recording devices,
- 20 questions about electronic spam mail,
- the rest of the calls did not concern matters in our competence.

We answer the questions more widely than our supervision competence would dictate. Concerning the publishing of personal data on the Internet, people are asking how to remove the personal data of their own or their close ones from search engines and social media. As a rule, the exercise of the so-called right to forgetting is a private law dispute where a supervision case is normally not initiated. Regardless, we explain what the persons themselves can do for their protection.

Concerning the requests for training and counselling, we have to make a choice because we cannot fulfil all requests. We base our choice on an impact assessment – when our contribution yields the most benefit. We conducted 18 training courses and 33 consultations to businesses and institutions last year.

A prioritised field in this context has been e-commerce. Good co-operation has been established with Estonian E-Commerce Association and the Consumer Protection Board.

We have also trained the public sector (personal data, public information, access restrictions), incl. in co-operation with the State Information System Authority (the National IT-Authority).

In awareness-raising work, we often use the help of partners and co-operation networks. I would like to mention co-operation with the E-Health Foundation and the Health Board in the field of the Internet forum for the protection of health data, the transparency and protection of persona data in government institutions - the network of chief privacy and transparency officers of governmental bodies, the data protection section of the Labour Inspectorate's work life portal, and our expert contribution to the projects "Nutiturva 2017" ["Smart Security"] and "Targalt Internetis" ["Smart on the Internet"]. ".

About preventive supervision

In addition to investigating individual violations, we try to have a wider impact on the protection of private life and the accessibility of public information by performing preventive supervision.

So, we conducted 14 comparative monitoring last year – assessing a total of 412 enterprises and public sector bodies. We send a summary of the monitoring together with the main conclusions to all participants. We usually make suggestions and recommendations based on the monitoring, as well as supplement our manuals. In case of more serious problems, we react with precepts.

The largest of last year's monitoring concerned the publishing of information on the websites of 213 local self-governments (municipalities). Upon preparing the checklist, we consulted with the Estonian Association of Rural Self-Governments and the Association of Estonian Cities, to be able to focus on practical problems. Based on the monitoring, the Inspectorate's advisory committee chose the municipalities of Halinga and Jõgeva as the local self-governments with the best online information. We conducted a similar monitoring for 15 county administrations.

The monitoring also concerned:

- the general terms of digital TV service providers (5),
- the use of telematics services (car-tracking) in private businesses (8),
- the deletion of personal data at the sellers of used electronic equipment (10),
- the data protection of communications enterprises (7), e-stores (10) and e-school information systems (3),
- the collection and use of customer data in banks (15) and sports clubs (12),
- the collection and use of data about private person debtors in debt collection enterprises (20),
- the implementation of access restrictions in the public document registers of schools (60).

In co-operation with the data protection inspectorates of Latvia and Lithuania, we monitored the processing of personnel data in the biggest store chains of the Baltic republics (4 in Estonia).

Last year's joint initiative of the Global Privacy Enforcement Network (GPEN) called the Internet Sweep Day focussed on the online safety of children; a total of 1,494 websites and mobile applications were monitored all over the world. The Inspectorate monitored 30 popular mobile applications in Estonia.

As a new form of preventive supervision, we implemented circulars. If we discover a problem that may presumably concern all enterprises or public sector bodies, we send them explanatorily circulars without initiating an investigation. Last year, we sent 5 circulars to 149 addressees.

Another form of preventive supervision is data protection audits in enterprises or public sector bodies that are large or process sensitive data. We focussed on healthcare. We audited 22 health centres and family physician centres/practices, while the State Information System Authority provided its own input into the checklist. We also audited East Tallinn Central Hospital [Ida-Tallinna Keskhaigla] and Estonian part of the European Visa Information System.

About the handling of violations

When we initiate proceedings, we prefer finding as fast and sustainable solution to the problem as possible. Last year, we received a total of 446 complaints. We initiated 384 more supervising cases on our own initiative.

We made 299 recommendations (in simpler matters, without asking for feedback) and suggestions (awaiting feedback) and 77 precepts in the course of supervision. Precepts almost always contain a warning of coercive fine. As a rule, the precepts were fulfilled; we had to make good on our coercive fine warning on just one occasion last year.

We closed 16 misdemeanour cases last year. 14 of them ended with imposing a fine. Half the punishments were for the abuse of the right to professional access to personal data (primarily health data, the police's database, the Population Register). Half the punishments were for the disclosure of sensitive personal data in the web-based document registers of local self-governments – we have usually limited ourselves to just warning before, but as it turns out, the number of such violations has unfortunately grown.

We changed our practice regarding electronic spam mail – the menace showed a growth trend. An individual spam message is a minor violation, but there is an entire industry behind it. A single message is sent tens of thousands of times even in the small country that is Estonia. All in all, it pushes people away from the online economy. You trust your contact data to one business or leave them afloat in the cyberspace, and the flows of spam SMS and e-mails just don't seem to cease anymore.
For that reason, we decided to make a precept of general nature to the sender already for the first violation. For the second violation, we apply coercive fine. In the case of the third violation, we publish the violator in the blacklist on the Inspectorate's website. The blacklist is intended as a warning to those business who would or could order the spam sending of their advertisements from the violators. And it seems to work because the blacklist prepared last spring has not grown thus far.

About the background of data transfers to 3rd countries

If a business is sending the personal data of Europeans to another business outside Europe where the data protection level is insufficient, it needs the permit of a data protection institution. In 2000, European Commission and the United States of America signed a Safe Harbour agreement concerning data protection and the Commission acknowledged the existence of a sufficient data protection level in those business that joined the programme established on the basis of that agreement.

On 6 October 2015, European Court of Justice declared the Safe Harbour null and void. In February this year, the Commission and US government reached an agreement in principle. The final implementation is still ahead.

Some data protection institutions consider it necessary to apply sanctions to businesses that used the Safe Harbour programme and continue to send personal data to the US in that manner. The Inspectorate does not apply sanctions but awaits the entry into force of the new data forwarding agreement. The businesses that used the Safe Heaven programme acted in good faith and have not violated anything out of malice.
I also have to note with resignation that the discussion of the topic of transferring personal data to the US contains a notable amount of hypocrisy.

The Data Protection Inspectorate in 2016

Supervision over the keeping of databases and the protection of information with access restrictions

In my previous annual presentation, I wrote that there was a frightening lack of order in the registration matters of the public sector databases. I referred to wide-scale ignoring of the requirement of database pre-approval, the requirement to implement security measures and the requirement to audit data protection.

On 16 January 2016, the new law amendments entered into force that transferred the supervision over the keeping of the public sector's databases from the State Information System Authority to the Data Protection Inspectorate. We also received the budget funds for one additional job position. Moreover, the Inspectorate was expressly given the supervision competence over the protection of information with access restrictions (regardless of whether it contains persona data).

We signed a co-operation arrangement with the State Information System Authority as a cyber security and network security institution, in order to effectively help each other upon tidying the public sector's data management.

On 30 March 2016, I undersigned extensive amendments to the general manual on public information. Among the rest, we supplemented it with a chapter on the protection of restricted information. While there is a separate law and a detailed implementing regulation concerning the protection of national security secrets, there were no helping and standardising requirements concerning restricted information. The new chapter should fill that void.

This year's goal of the supervision of databases is to tidy the foundation of register management – the data about all databases, kept in the Administration System of the State Informa-

tion System. In February monitoring, we found that 138 of the state's 353 databases had the status "being established", while actually being already in use and interfaced to the data exchange layer of databases (the X-Road). We have started dealing with the violators under the supervision procedure.

Additionally, the Ministry of Economic Affairs and Communications asks us for information before deciding the allocation of funds for a database from the EU structural funds. Those ignoring the basic database hygiene requirements will not get any funds.

Healthcare and social sector

We started the preparation of the guideline of using and forwarding data about persons needing healthcare and welfare aid last year; due to an employee leaving, the completion of the manual was delayed until this year. The purpose is to provide a practical material to help those moving data about persons in need between institutions (the welfare and child protection workers of local governments, the police, schools, kindergartens, healthcare personnel, etc.). Information about a person in need must not be left stuck in one place while referring to data protection, but the data must be used securely in light of their sensitivity.

This year's plans also include the auditing of 24 general practitioners and the follow-up auditing of the e-ambulance system (at the time of the last year's audit, the e-ambulance system did not function satisfactorily).

Personal data in business and working life

We have already organised a round table with the developers of software solutions for e-stores. E-traders are normally using standard solutions, so with advising the software developers, any data protection problems can be prevented "in the bud". With the initiative and support of the Chamber of Commerce and Industry, a series of training courses on practical matters are planned for businesses.

The use of modern technology in customer and employment relations is planned to be covered with several activities this year. Probably the most extensive of those is joint monitoring with the Consumer Protection Board – we will jointly inspect at least 10 mobile applications for e-shopping. We will use the help of IT experts in that, to make sure that what is promised to the users of the services will also work in practice.

There are also plans to monitor the businesses collecting debts (debts' recovery companies, 10) and providing financial credibility ranking services (3). In insurance providers (14), we inspect the use of customer data in electronic direct mailing.

We contributed to the joint reminder of the Civil Aviation Administration and the Consumer Protection Board, teaching the safe and lawful use of flying and recording drones.

Personal data in internal security and law enforcement

We continue with the internal monitoring efforts initiated last year and the year before that in the area of government of the Ministry of the Interior. We also inspect the Punishment Register (Criminal Records Register) and the public part of the Courts Information System.

Cover adjudications, a strange situation has appeared after the Supreme Court's 11 May 2015 judgement No. 3-3-1-90-14. On the one hand, the opinion of a higher court says that we do not have the supervision competence over courts (court chancelleries) anymore, after the state

supervision was divided into state supervision and administrative supervision. But on the other hand, we continue to have the right to proceed misdemeanour cases concerning court officials under the same circumstances where we do not have the supervision competence anymore. The Ministry of Justice has promised to find a solution to that legal confusion.

Public sector information

Concerning the accessibility of public information, we continue the monitoring of online information of institutions. Due to the added supervision competence over the protection of information with access restrictions, we also conduct on-site inspection visits. We will organise a larger information day for the implementers of the law in co-operation with the State Information System Authority.

We also monitor the functioning of the new provisions of the Public Information Act about the establishing of licenses for the re-use of information, the taking of service charges and the limitation of personal contact data, which entered into force on 16 January 2016.

International co-operation

Estimably in the end of the first semester of 2016, European Union's General Data Protection Regulation on personal data protection together with its Data Protection Directive in the field of law enforcement will be adopted. They should enter into force in the end of a 2-year transition period. This means extensive preparatory work both in the European working party of data protection authorities and at the country level.

Most important recommendations in 2016

Recommendations for businesses

a) Account for data protection in IT product development right from the start.

The IT sector and especially start-up businesses are always developing new business products based on smart collection, analysis and forwarding of personal data. A start-up business is founded to develop a product as quickly as possible. We recommend thinking through the risks to people's private life and account for the data protection requirements right from the start. This way, the product will be more valuable, while ignoring this makes for additional expenses or even failure.

Useful material is available at the Inspectorate's website, among other places. We may not have enough resources to advise every project in detail but we are always willing to organise seminars on practical matters in co-operation with professional associations and the Chamber of Commerce and Industry;

b) The keepers of registers of debts are responsible for the identification of justified interest to view and for the inspection of the data's correctness.

The law sets out the following obligations for the keepers of registers of debts: 1) to verify the correctness of the debt data, and 2) to identify the viewer's legitimate interest to view the data of the specific person (Personal Data Protection Act, § 11 (6)).

Unfortunately, service providers tend to ignore those obligations, limiting their activities to merely cashing in the fees. All responsibility for their obligations is pushed onto the shoulders of the viewers, and disputes are sent to the Inspectorate. We issued a preliminary warning to the relevant service providers with a circular, pointing out that such a business model is illegal.

We would like to repeat here that if a service provider ignores its obligations, we will apply sanctions not to the viewer but to the service provider enabling the option to view the data;

c) Avoid a central database when creating a positive credit register, and restrict queries so that they can be made only if filing a loan application.

The businesses of the financial sector and also the Ministry of Justice are discussing the possibility of creating a positive credit register, containing not only negative information (payment problems) but also positive information (all payment obligations to the maximum extent possible, or their absence).

This is a welcome thing if it makes the credit market more favourable to the consumer – helps lower the interests and enliven the competition. But the idea entails two risks. First, the risk of abusing the right to access the information, and second, the risk that the discovery of all payment obligations of a person would lead to more aggressive sales work increasing the number of people ending up with payment problems ("*You still have 20% to go until the payment ceiling of your loan obligations, take another loan!*"). To hedge those risks, we recommend:

- not creating a central database but instead a secure query option across the databases of the relevant credit institutions, similar to the X-Road (every business itself keeps careful watch over the use of its data),
- permitting queries only if the person is applying for a loan, not for credit enterprises to make loan offers of their own,
- clearly setting out the limited circle of businesses having access to the data.

Recommendations to public sector bodies

d) To all public sector bodies: use the official e-mail address as the first choice in correspondence.

The official e-mail address (personal ID code@eesti.ee, registry code@eesti.ee) is set for every Estonian citizen, resident, e-resident and legal person. I recommend using this as the first choice in correspondence. It is secure and makes for faster procedures. Those who have set it upon for themselves or entered their mobile telephone number in the state information portal have also accepted the terms of use of the official e-mail. Pursuant to those terms, the person grants a general future-oriented consent to the serving of procedural documents if the consent is required pursuant to the law. Naturally, the official e-mail address can also be used for sending the person ordinary notices and letters not subject to the legal requirement of serving.

e) To all public sector bodies: take an inventory of access to information and restrictions of that access, and anonymise the web-based document register.

We also presented those two recommendations last year and the year before, and they are still relevant today. But the amendment to the Public Information Act that entered into force on 16 January 2016 (§ 3.1 (3), § 12 (3.1)) made those two recommendations obligatory;

f) To all public sector bodies: put your database keeping in order, and quickly.

We pointed out in the last year's annual presentation that the general requirements for keeping databases (Chapter 5.1 of the Public Information Act) were being ignored on a wide scale. Starting with 16 January 2016 the supervision over the keeping of databases has been given to the Inspectorate. The Inspectorate and the State Information System Authority co-operate to tidy the register management. We strictly recommend that all keepers of public sector databases:

- immediately correct the registrations of their databases in the state information system's administrative system;
- use only the X-Road for data exchange between databases, including exchange between the institution's own databases (§ 43.9 (5) of the Public Information Act). The X-Road is secure, leaving a trail of all activities;
- I additionally recommend that the monitoring of anomalies be automated in databases with sensitive content and a wide user base in order to detect abuses, and that archiving and deletion be automated in large databases;

g) To the Ministry of Social Affairs:

- before adding new user types and new data types to the e-health information system, tidy the existing ones. The following needs to be ensured: a) the quality of the data (the information being collected is far from being wholesome), b) the protection of the data from abuse, c) the lawfulness of keeping the database (incl. that the interfacing of the e-prescriptions database has no legal basis);
- the preservation of the documents left after deceased/dissolved providers of healthcare services must be solved. It is not enough to establish the time limits for preservation if there is no factual mechanism to ensure the preservation;
- sensitive unemployment data being added to the Unemployment Insurance Fund's information systems need effective internal auditing to prevent abuse;

h) To the Ministry of Justice: the Public Information Act enables the setting of an access restriction on information for 5 years and to extend it once for 5 years. An exception to that is personal data, to which a so-called lifetime restriction can be set. I recommend that it be considered whether the 10-year maximum time limit is enough for a description of security measures, as well as for several national security restrictions and information endangering the preservation of a species under nature protection (§ 35 (1) 4), 5), 5^2), 6), 6^1), 6^2), 9) of the Public Information Act). Certainly, no blanket extension of the time limits must take place; in most cases 5+5 years are fully sufficient. Yet, in certain cases where the information definitely needs to be protected after the passing of 10 years as well, the information holders will start to simply destroy the information when the access restriction limit is passed, or will try to make it a state secret.

Respectfully,

Viljar Peep
Director General, Data Protection Inspectorate