OVERVIEW AND RECOMMENDATIONS FROM THE DIRECTOR GENERAL

Becoming a digital society

Data protection law was created as a reaction to the development of information technology – to mitigate the risks it poses. This development keeps accelerating. Our daily lives are becoming increasingly networked in a global computer network. Data analysis and auto-profiling, among others, are used more and more.

In terms of IT development, this year and the last have been of great significance in Estonia:

- March 2017 saw the launch of testing of self-driving vehicles, which the working group of the Government Office compiled greenlighted with a final report titled "The start of the age of self-driving vehicles", on the condition that a person responsible is in the vehicle and can take over steering.
- On-demand ride sourcing, i.e. ridesharing, was regularised on 14 June 2017. The development of information technology takes the models of sharing economy to the fields of transport and accommodation among others.
- Parcel robots that drive on roads and sidewalks were granted protection by law on the same day. Drivers are now required to pay robots on pedestrian crossings just as much attention as they do to cyclists.
- On 16 June 2017, the Estonian and Finnish Governments established a joint institute for the cross-border use of their data exchange layers (X-Road). X-Road is a solution that was created in Estonia and that allows for secure transfer, encryption and time stamping of data. This creates a new level for cross-border use of data between countries (population registers, tax administrations, etc.).
- On June 20, the prime ministers of Estonia and Luxembourg signed an agreement to establish the world's first data embassy. Backups of information systems that are essential for the functioning of the Republic of Estonia will be duplicated in a secured data centre located in the Grand Duchy of Luxembourg.
- We also had our first big cyber scare as a security threat of the ID-card chip software was disclosed to the public in September. Fortunately, the threat remained merely theoretical. Therefore, we continue to have the world's best management solution for digital identity and the most extensive daily use of digital identity (proportionally).
- In March 2018, the Government Office and the Ministry of Economic Affairs and Communications decided to convene an artificial intelligence working group. The objective of the working group is to compile both legal solutions (AI legislation) and the corresponding national strategy. How to regulate responsibility when a self-learning device makes independent decisions that the creators of the algorithm can no longer foresee?

Estonia is one of the pioneers in the IT development of the world. The fact that line is not an empty phrase was made very clear to me in September 2017, in Hong Kong, at the

International Conference of Data Protection and Privacy Commissioners, the opening panel of which I attended to introduce e-Estonia.

Naturally, information security and the proper collection and use of personal data are currently more important than ever before.

New data protection law from May

As of 25 May 2018, the General Data Protection Regulation be implemented and it will be directly applicable in all Member States of the European Union. More than a hundred Estonian legislative act will be amended in connection with the implementation of said regulation. The new Cyber Security Act will also come into force in May. What these news mean to computer folks is that updating the operating system is necessary both for the use of personal data and to ensure information security.

Why is all this necessary? Fortunately, Estonia has managed to avoid the most significant international malware outbreaks and misuse scandals concerning personal data so far. But more and more of life is moving into cyberspace and that includes the bad gays. Aiding the improvement of information management and security will benefit our companies and public authorities as it enables us to:

a) protect our information assets better,
b) be more efficient and competitive in our work and
c) be more reliable for citizens/clients/employees.

It is not possible to develop e-services successfully, neither in the private or public sector, if people do not trust the ways in which their personal information is stored. The new acquis should reinforce peoples' control over their own data.

Should we expect massive fines?

High fine levels set out in the General Regulation have received a great deal of attention. Several trainers and consultants have highlighted this when promoting their services.

Yes, it is true that the provisions of the General Regulation concerning the activities of data protection authorities are focused on complaints, violations and punishment. Nevertheless, I can confirm that we will not become transfixed on writing out fines as of 25 May. Unlike a number of other Member States, the Estonian Data Protection Inspectorate has always had the right to enforce sanctions. Relevant practices have been developed during two decades and no fundamental changes are likely to occur.

The Inspectorate has been focused on prevention and awareness raising. In the case of violations, our main pattern of behaviour has been providing explanations and warnings. We use sanctions and duress as a last resort. There are two reservations to this:

1) our small size brings sets restrictions in providing clarifications and explanations – the possibilities for thorough explanation on a single company/institution level are relatively meagre,

2) in the case of maliciousness, as well as repeated serious violations, there is no use in warning and giving new opportunities; in such cases, a strict approach is appropriate.

What shall the inspectorate do for the implementation of the new data protection law?

We have three priority objectives.

1. Fulfil the obligations of a data protection authority of a Member State, arising from the new regulation (21 specific tasks and 26 authorised powers).[1] Preparatory work in Estonia as well as in the European working party has been extensive (creating guidelines, awareness raising activities, updating the information system, changes in organisation of work).
2. At the same time, the General Regulation offers opportunities for balanced and flexible implementation. These opportunities should be used in light of Estonia's digital development, the openness of society and the small size of businesses and agencies. I have, on behalf of the Inspectorate, submitted relevant legislative proposals to the Ministry of Justice and I am ready to explain those during proceedings in the *Riigikogu* (Estonian Parliament) as well.
3. We will use the new data protection and cyber security law to improve the level of information management and information security in Estonian companies and agencies – we will increase our competitiveness, prevent new threats and create new opportunities.

Summary of activities in 2017

When it comes to numbers, the previous year can be summarised as follows:

PERFORMANCE INDICATORS	2014	**2015**	2016	**2017**
Creating guidelines, policy advice				
guidelines (excl. updating existing ones)	6	**4**	1	**2**
opinions on draft legislation	28	**35**	27	**34**
Awareness raising				
questions	1144	**1369**	1417	**1520**
phone calls to the help line	1,141	**1,136**	1,419	**1,527**
ad hoc consultations (for companies, agencies)	34	**33**	79	**148**
training courses (organised or took part as a lecturer)	24	**18**	23	**17**
Monitoring				

[1] See articles 57 and 58 of the General Regulation.

Circulars (without investigation)	-	**5**	5	**4**
incl. the addressees of the circulars		**149**	34	**26**
large scale comparative monitoring	6	**14**	9	**10**
incl. those monitored		**412**	148	**129**
complaints, appeals (submitted)	413	**446**	390	**462**
self-initiated supervision cases (initiated)	152	**384**	86	**149**
incl. preventive data protection audits	16	**24**	24	**1**
on-site inspections (within supervision cases)	48	**35**	33	**45**
recommendations and proposals (within supervision cases)		**299**	56	**125**
precepts/injunctions (usually preceded by a proposal; as a rule, including a coercive fine warning)	86	**77**	59	**64**
incl. registration (without previous proposal)	45	**28**	26	**35**
misdemeanor cases (completed)	11	**16**	16	**9**
penal law fines (misdemeanor penalty), administrative law fines (coercive fines)	8	**15**	16	**4**
Authorisation and special procedures				
applications for registration (for the processing of sensitive data or for determining the responsible person)	902	**540**	547	**641**
requests for the coordination of databases (for setting up, implementing, changing the data set, terminating)	115	**167**	139	**99**
applications for research without the consent of data subjects	13	**29**	18	**54**
applications for transfer of personal data to a foreign country	13	**8**	18	**22**
applications for one's own data in the databases of Schengen, Europol, and other cross-border databases	6	**10**	10	**8**
Employees and budget of the institution				
statutory positions	18	**18**	19	**19**
annual budget (thousand euros)	654	**671**	700	**714**

These numbers represent all the work my colleagues have done during the year. In the following chapters, they will analyse their areas of responsibility in greater detail by themselves, describing the most important feats of the year. I will touch upon a few events and developments.

Legislative drafting

On 23 March 2018, the Ministry of Justice submitted a new draft of the Personal Data Protection Act to the government, and amendments to other acts were submitted for coordination to other ministries on the same day. The comments of the Inspectorate to the draft acts and other materials have been published on our website, in the reform section.

I proposed, in the annual report for 2013 (p. 18, cl. 1) to update the rules governing the delivery of procedural documents. The Administrative Procedure Act stipulated prior consent for electronic delivery, unlike in the case regular mail (in paper format). The official email address (personal or registration code@eesti.ee) did not hold any legal significance. Instead of using contact information from the main registry (population and commercial register), authorities collected contact information by individual procedures. This led to delays in procedures, high postal expenses and poor quality of the contact information. With approval from the secretary generals of the ministries concerned, I convened an informal working group in September 2013. Our proposals came about as a result of the energetic work of the Legislative Policy Department of the Ministry of Justice only four years later – the draft Administrative Procedure Act was submitted in August 2017 and adopted in December.

Access to public information, information protection at the Data Protection Inspectorate, maintaining databases

On the basis of the "Principles for Managing Services and Governing Information" regulation, a Public Information Council, the members of which are representatives of ministries and other central authorities, was created at the Inspectorate. This allowed us to coordinate both access to public information and work related to the protection of personal data in the public sector.

Last year, we inspected the protection of information with restricted access at 10 agencies, accompanied by the Information System Authority (the national IT and cyber security authority) in six cases. Fortunately, no significant shortcomings were discovered. During the second half of this year, we plan to launch "fire drills" – unannounced visits to a establishments where we will evaluate the readiness for crisis response and the instructions that the staff has been given.

In January 2016, the Inspectorate took over the supervision of the databases. Last year, the number of databases, the adoption of which has been coordinated, increased from 277 to 539. However, this does not indicate a sharp increase in the number of databases, but instead is proof that public authorities began to comply with the requirements for the coordination of databases.

Finance sector

One of the most interesting self-initiated monitoring cases in 2017 was the monitoring of mobile applications used in online banking. It got started from a suspicion that one application might make it possible for the bank to access business clients' phonebooks without parties involved having any knowledge of this. Fortunately, this suspicion was not confirmed. One of the eight banks monitored did gain access to the phonebook of a client's telephone, but used contacts with consent from the persons who had signed up for the service.

Acknowledgements

2018 is a very special year, not just for the Republic of Estonia, which recently celebrated its Centenary, but also for the field of data protection. The new data protection law contains a lot of uncertainty. The preparatory work, conducted both in Estonia and the joint body in Brussels, is vast in volume. The delayed completion of the European-wide guidelines and the national implementation laws have hindered preparations.

This makes for even more reasons to thank my colleagues. We are working in stressful, but fascinating times. You have put your hearts into your work and done it exceptionally well. And for this I am truly grateful to all of you! Together, we have set up an institution that keeps a balance between the protection of fundamental rights and public interests. We do not look for obstacles so that we would have something to do, instead we seek out solutions so that the necessary tasks would get completed. We are focused on what is important, so that we are able to see the forest through the trees.

I would also like to thank the Advisory Council members of the Inspectorate, who have contributed their time to discussing issues concerning data protection and public information. I am grateful to the members of the Public Information Council for the experiences they have brought along from their jurisdictions. I extend my gratitude to superb colleagues from ministries, agencies, municipalities, the Estonian Chamber of Commerce and Industry and from all other partner organizations.

From among our cooperation partners, I would like to highlight Tallinn University of Technology, Tallinn University, University of Tartu and Tallinn School of Economics for their fast launch of refresher courses for data protection officers. Data protection and information security are fields where greater professionalisation is needed when compared to the current levels. Your work has contributed to this significantly.

RECCOMMENDATIONS

Recommendations to a head of a company for the implementation of the new data protection law

As of May 25, 2018, the General Data Protection Regulation must be implemented in all countries of the European Union. For this end, I recommend:

1. Everything starts with people - make sure that your company has the necessary expertise in data protection and information security (among your staff or from outside). However, keep in mind that it is not the data protection officer who is liable, instead it is the Management Board of the company – just as in the case of accounting or tax obligations.
2. Organise for the mapping of existing information assets in order to compile/update documents that are linked to one another:
    a) a balance-like data processing register pursuant to article 30 of the General Data Protection Regulation (the Inspectorate has the right to request it, simpler samples can be found on our website)
    b) data protection conditions targeted at clients and partners, pursuant to article 12 of the General Regulation,

c) if you are a service provider listed in the Cyber Security Act, then a risk assessment for taking security measures.

3. On the basis of that mapping, you can take necessary measures to be prepared for:
    a) inquiries concerning peoples' own data,
    b) data portability requests,
    c) submission of violation notifications about significant violations concerning personal data through the Inspectorate's website,
    d) if you are a service provider listed in the Cyber Security Act, then for notifying the Information System Authority of cyber incidents as well.
4. If there are any loose ends concerning data protection in your field of activity, conduct cooperation through your business or professional association and compile guidelines for good practices. Cooperation enables you to compile materials that bring the most benefits. The Inspectorate's ability to advise in greater detail on individual level is relatively meagre, but we are happy to help on a sectoral level.

Recommendations to a head of a public sector body for the implementation of the new data protection law

1. Everything starts from people – make sure that your institution has a competent data protection officer and a head of information security (either among your staff or external officials). However, keep in mind that it is not the data protection officer who is liable, instead it is the head of the institution – just as in the case of accounting or tax obligations.
2. Organise for the mapping of existing information assets in order to compile/update documents that are linked to one another:
    a) a balance-like data processing register pursuant to article 30 of the General Data Protection Regulation (the Inspectorate has the right to request it, simpler samples can be found on our website)
    b) impact assessment of open data pursuant to § 3^1 of the Public Information Act (why and how your institution provides or does not provide your public digital database in the form of open data),
    c) data protection conditions targeted to the public in accordance with article 12 of the General Regulation,
    d) risk assessment for taking security measures pursuant to the Cyber Security Act,
    e) an overview of information assets pursuant to § 12 of the "Principles for Managing Services and Governing Information" regulation,
    f) document classification scheme according to §§ 6–8 of the "Archive rules".
3. On the basis of that mapping, you can take necessary measures to be prepared for:
    a) inquiries concerning peoples' own data,
    b) submission of violation notifications about significant violations through the Inspectorate's website,
    c) reporting of cyber incidents the Information System Authority.
4. Let your officers follow the work of the Public Information Council work (joint body of representatives of national central authorities in the field of public information and personal data protection). If you are a public authority, ask for advice from your ministry representative at the council, if necessary. If you are a municipal employee, you can also

get practical advice from Tallinn City Government and the Türi Municipality Government, which, in cooperation with the Inspectorate, are piloting the implementation of the new data protection law. Tallinn is part of the council as a representative of local governments.

Recommendations to the Ministry of Justice

1. I agree that the Sanctions chapter of the draft act of the new Personal Data Protection Act has failed. Firstly, the European legislature is directing high fines at the private sector; whereas, pursuant to the draft act, violations of the same content are non-punishable in the public sector. That is neither reasonable nor just. As an institution cannot be fined, the misdemeanour liability of an official should be applied. Secondly, I think that the time is ripe for the restoration of administrative fines of legal persons in the Estonian legislation. The sanctioning of legal persons through the current misdemeanor procedure is terribly ineffective and burdensome to all parties. More detailed proposals have been submitted separately.[2]
2. I would like to repeat the problem with mass inquiries that was touched upon in last year's presentation (see page 11). I am referring to the possibility where a law enforcement agency can set up a machine to harvest information on people from across databases and this activity has legal consequences for the object of harvesting.[3] It is completely unacceptable to use general rules meant for individual inquiries for automated mass inquiries. The Tax and Customs Board has appropriate rules for risk assessment, i.e. tax fraud detection. Automated mass inquiries are also spreading to other areas. On 14 March 2018, the Parliament adopted supplementary provisions to the Social Welfare Act in order to determine unemployed young people. In my estimation, the supplementary provisions are limited when it comes to activities following the inquiry. I would like to point out to the Ministry of Justice that the requirement of the General Regulation that if the national legislature provides for making individual decisions based on automatic data processing, then it must also provide appropriate protective measures.[4] The use of data analysis in public administration is increasing, so hiding one's head under the sand is clearly not an option. Supplementing the Law Enforcement Act in terms of such monitoring measures is vital.
3. How public is the data concerning wages in the public sector? The wages of officials are published online, but can a request for information be made to see the wages paid out of the public budget under an employment contract in personalized form? The interpretation of the Inspectorate that it is possible pursuant to § 36 (1) 9) of the Public Information Act has been repeatedly contested. The legislator should express their will clearly on such an important issue.

[2] Exhaustively described in the letter sent on 16 October 2017. The same problems have been outlined on in the overview (III-10) published on 14 October 2016, in viewpoints (chapter 2) published on 27 April 2017 and the memo on administrative fines published on 29 May 2017.
[3] In this case, I do not refer to statistical data analytics, because that does not lead to consequences for those investigated – the monitoring results in non-personalized generalizations.
[4] Article 20 (2) (b) of the General Data Protection Regulation.

Recommendations to the Ministry of Economic Affairs and Communications and the Information System Authority

1. From the viewpoint of legal rules, the protection of personal data and cyber security are presented like two distinct fields with two separate supervisory authorities. However, for the end-user (company and public sector body), they are largely overlapping, especially with regard to information security. The central implementation manual of information security, the three-level IT baseline security system (ISKE), does not currently contain protection of personal data. I recommend that the corresponding parts be added. The Ministry of Justice has adopted data protection module of the ISKE source material (IT Baseline Protection Manual of the German Federal Office for Information Security) to Estonian context.

   I maintain that ISKE is a great tool for large organisations. Certain smaller data processors need simpler guidelines, which have been compiled specifically for them e.g., local governments and other smaller institutions, general practitioners (family physicians) and other smaller healthcare providers.

2. Correspondence between individuals and authorities has moved from the regular mail to e-mail. I recommend preparing for the next stage – directing correspondence to a web application. A private person could use this to get a comprehensive overview when reviewing their inquiries and would not have to look for those in the registers of documents of various institutions. The register of documents includes a reply term and the name of the reviewing unit/institution, but since the name of the inquirer has to be replaced with initials, that is of little use. A personal “desktop” that one can log into would be a better solution for an inquirer. The institution has to do a lot of manual work, which could be automated with the use of a web application. The Inspectorate is currently working on creating its own web application. I would recommend that the same model be used in general as well – requests for clarification, memorandums, requests for information, complaints and the like are handled similarly in public institutions.

Viljar Peep PhD
Director General of the Estonian Data Protection Inspectorate