YEAR 2018 THROUGH THE EYES OF THE LEGAL DIRECTOR

Overview of the activities of Estonian Data Protection Inspectorate and recommendations for year 2019

2018 has been a year of changes in many ways – for the Data Protection Inspectorate, personal data controllers and processors, as well as data subjects. As is known, amendments were made in the regulations of personal data protection when the General Data Protection Regulation (regulation (EL) 2016/679 of the European Parliament and of the Council) (hereinafter GDPR) came into force. Besides that, Member States of the European Union had to also adopt the so-called Law-Enforcement Directive (directive (EL) 2016/680 of the European Parliament and of the Council) – a legal act regulating the activities of law-enforcement authorities in preventing, detecting and prosecuting offences and executing criminal penalties .

The updated regulations strengthened the requirements of personal data protection. Some of the previously in-force data processing principles were turned into legal provisions. For example, the principles of data protection by design and by default were established as separate requirements.

Taking it all into account, it was difficult to create an overview of 2018. The Inspectorate had many new topics and activities, making it impossible to give an overview of all changes in this annual report. We will focus on the most important changes that the GDPR and Law Enforcement Directive entail. First we will discuss situations which are from now on a little different, or which in our opinion need to be explained more.

For example, we need to address the topics of data protection risk and impact assessment, nature and necessity of data protection officers, as well as submitting a violation notice in the case of breach of personal data processing.

We will mention changes in situations where personal data is sent to third countries. In addition, we will write about some of the problematic areas in the field of public information. One part of it is connected to private holders of public information who cannot determine when they are the servers of public function and therefore holders of information. There are situation, where public authorities also do not fully know which public function is served by the legal person governed by private law that they have created. We will also mention problems in regard to fulfilling information requirements and concerns related to

document registers. We will give an overview of inspections of local governments – both the on the spot investigations as well as website monitoring.

In the overview, we will give brief explanation how electronic contact details can be used to conduct direct marketing – chiefly, whether the GDPR changed something in regard to this or not.

We will mention separately an overview of some proceedings. For example, we noticed that in the field of employment relationships, the activities of personal data processing are not organised sufficiently clearly and transparently – especially in situation where the employer has not established the terms for personal data processing. On several occasions, we also dealt with proceedings where there were no legal basis for disclosing personal data or accessing data (for example, misuse of access to health information system). In addition, there were proceedings where it was thought that the GDPR gives an opportunity to delete all personal data, even in cases where a person has debts.

In addition, we will give a short overview of draft legislations that were submitted for feedback from the Inspectorate, which the Inspectorate gave. We can see a tendency in regard to drafts that were included in this annual report as well as not included, where all circumstances are not always thought through when drafting a legislation. This does not only concern draft legislation but we see similar mistakes in amendments of database statutes.

After the GDPR came into force, we often received drafts which did not mention in any way the data protection impact assessment. Impact assessment should be one part of the explanatory memorandum of the draft, but unfortunately, it was not always included, even though this obligation is set out in the GDPR.

Based on drafts received in the last year for feedback, it can be concluded that the state wishes to use more technological solutions for fulfilling its functions. They want often to process large sets of data, whether the purpose is making some decisions or conducting investigations. It is understandable that new technological solutions evolve services and help to make decisions, but a controller or processor is not allowed to act without being sure of the rules and making data processing transparent. For example, appropriate measures need to be taken in order to protect the rights, freedom and legitimate interests of people when making automatic decisions, including profile analysis. For the public sector, automatic decisions need to be regulated on legislation level. It all means that indiscriminate mass-processing of personal data is not allowed.

You will also find in the overview of the year's activities separate chapters on cross-border collaboration – participation in international workgroups and cooperation with other supervisory authorities. In general, it can be said that the cooperation of the Inspectorate with other data protection supervisory authorities has increased and the tendency in regard to this continues.

In the last year, we had to constantly introduce and explain the requirements of the GDPR. Explanatory articles on the GDPR were also gathered into a general guideline for controllers and processors of personal data, which we published on 31 May 2018.[1] The guideline is meant as a practical material for all controllers and processors – companies, non-profit associations, authorities, officials. The general guide does not include recommendations in more specific areas. For that, the Inspectorate has thematic guidelines, which are being updated.

Statistical indicators

Last year, our performance indicators increased (see for example advice line indicators). We believe that this was caused by the changes in data protection laws. The next page includes a comparison of statistical performance indicators over the last four years, and the last chapter of the annual report includes a detailed overview of the activities of the last year. In conclusion, our work volume increased – despite the fact that we had an objective to decrease the amount of self-initiated investigations in the last year.

[1] The general guide for a personal data processor can be found here: https://www.aki.ee/et/juhised.

Comparison of performance indicators over the last four years

PERFORMANCE INDICATORS	2015	**2016**	2017	**2018**
Creating guidelines, policy advice				
guides (excl. updating existing ones)	4	**1**	2	**1**
opinions on draft legislation	35	**27**	34	**42**
Awareness raising				
requests for clarification, memorandums, claim letters, requests for information	1,369	**1,417**	1,520	**2,384**
calls to the help-line	1,136	**1,419**	1,527	**2,556**
consultations (for companies, institutions)	33	**79**	148	**200**
training courses (organised or participated as a lecturer)	18	**23**	17	**23**
Supervision				
circulars (without initiating supervision)	5	**5**	4	**8**
incl. the addressees of the circulars	149	**34**	26	**162**
large scale comparative monitoring sessions	14	**9**	10	**2**
incl. no. of monitored	412	**148**	129	**85**
complaints, challenges, misdemeanour notices (submitted)	446	**390**	462	**462**
Complaints, requests for clarification, breach notifications, memorandums, permit and notification proceedings via IMI (EU information system through which data protection authorities exchange information)	-	**-**	-	**479**
self-initiated supervisory cases (initiated)	384	**86**	149	**15**
incl. preventive data protection audits	24	**24**	1	**1**
on-site inspections (in supervisory cases)	36	**33**	45	**17**

PERFORMANCE INDICATORS	2015	**2016**	2017	**2018**
Monitoring				
recommendations and proposals (in supervisory cases)	299	**56**	125	**10**
precepts (usually preceded by a proposal; as a rule, includes a coercive fine warning)	77	**59**	64	**46**
incl. registration (without previous proposal)	28	**26**	35	**-**
misdemeanour cases (closed)	16	**16**	9	**23**
penal law fines (misdemeanour penalty), coercive fines (in supervisory proceedings)	15	**16**	4	**9**
Licensing and special proceedings				
registration applications (for prior checking of processing of sensitive data or appointing a data protection officer) – DIATR was closed on 24 May 2018	540	**547**	641	**192**
submissions for database approval (for establishing, taking into use, changing the data set, ending)	167	**139**	99	**36**
submissions for licences for scientific research without the consent of the data subjects	29	**18**	54	**61**
submissions for licenses for data transfer to a foreign country without adequate data protection level	8	**18**	22	**3**
submissions for one's own data in the databases of Schengen, Europol, and other cross-border databases	10	**10**	8	**21**
The number of employees of the Inspectorate and its budget				
statutory positions	18	**19**	19	**19**
annual budget (thousand euros)	671	**700**	714	**717**

Activities of the Data Protection Inspectorate in 2019

It is impossible to foresee the future, which means that all of our activities of 2019 cannot be foreseen. Therefore, we can mention only activities which we have definitely taken into account.

- We will conduct procedural cooperation with both other data protection supervisory authorities as well as national authorities like the Information System Authority of Estonia.
- We will continue raising awareness. We will conduct prevention and awareness raising activities within our means, taking into account the trends and problems that the society has.
- We will prepare for new supervision. The Inspectorate has been given an obligation to monitor the webpages and mobile applications of information holders of the public sector as well as private entities and persons that perform public functions or in other words information holders governed by private law, and make sure that the pages and applications correspond to the requirements of the so-called Accessibility Directive (directive (EU) 2016/2102 of the European Parliament and of the Council) – for that reason, we are preparing for the supervisory task.
- We will update the guides and illustrative materials of the Inspectorate.
- We will participate in the work of European Data Protection Board, including creating related guidelines.

One might ask when will the Data Protection Inspectorate start imposing "huge fines", established by the GDPR, which according to the Estonian legislation have to be handled within the misdemeanour proceeding. Rest assured, the Data Protection Inspectorate will not become a fine factory. We have had the option of imposing sanctions even before the GDPR. The related practice has established itself over the years and we foresee no fundamental changes. In the case of violations, our main pattern of behaviour has been providing explanations and warnings. We use sanctions and compulsion as a last resort. At the same time, this does not mean that in the case of malevolence or a repeated serious violation, we will only give out warnings and a new chance.

RECCOMMENDATIONS FOR 2019

In this subchapter, I will give recommendations to lawmakers, controllers and processors for improved application of personal data protection regulations as well as norms in regard to public information.

Several recommendations are similar to those in 2017 overview, but I believe that it is necessary to repeat and remind them.

Recommendations to a head of a company

- **Establish** clear, simple, and understandable terms for personal data processing – both for clients and your employees.
- **Make sure** that the company's employees have undergone trainings, received explanations and (written) guidelines which help them to legally process personal data on behalf of the company.
- **Map the necessary information assets**, including balance-style data processing register, which would first and foremost give an overview of processed personal data and the legal basis for their processing. If you are a service provider listed in the Estonian Cyber Security Act, then create a risk assessment for taking security measures.
- **Before you begin** a new type of personal data processing for the company, conduct a written data protection impact assessment. If this new type of personal data processing is related to a situation where, due to changes in legal acts, the company is given additional rights or possibilities for processing personal data, check whether the explanatory memorandum of the draft legislation includes a data protection impact assessment. If the explanatory memorandum of the draft legislation has no such analysis or if it does not cover all planned personal data processing activities, conduct a data protection impact assessment.
- **Be prepared** for situations where a data subject wishes to see his/her personal data, requests that they be amended, deleted, their processing restricted, wishes that they be transmitted or wishes to give objections. If you amend, delete or restrict the processing of personal data, then be prepared to notify the recipients who received the personal data from the company.

- When forwarding data to third countries, **clarify** whether there is a suitable legal framework for this – for example, there is a decision of the European Commission on the sufficient level of data protection, when to use appropriate safeguards or binding corporate rules, or when the personal data are transferred according to derogations for specific situations. Considering the current situation, this has to be also clarified in a situation, where personal data are forwarded to the United Kingdom – especially in the case of no-deal Brexit.

- **Implement** relevant and necessary security measures to protect personal data.

- **Make clear early** in which violations of personal data processing you are required to notify the Estonian Data Protection Inspectorate within 72 hours. In some situations, the data subjects and the Information System Authority of Estonia have to be notified.

- **Establish** and implement internal control mechanisms in order to discover the violations of the requirements of personal data processing in your company.

- **Prepare for** cooperation with an association of businesses or a professional unions in order to create guidelines for best practices or codes of conduct. If the company's field of activity has loose ends in regard to data protection, then it is possible to jointly create a code of conduct for best practices. By knowing one's area better, it is possible to create materials which are hugely helpful. 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.

- **Clarify** whether the company has a public function, which makes it a holder of information pursuant to the Public Information Act. For this we recommend to check relevant administrative contracts, initial documents of establishing a company, and articles of associations, as well as other documents related to establishing a company and transferring a possible public function. This determines the extent to which the activities of the company are governed by the requirements of the Public Information Act.

- **Check** whether the company has been given a public function. If yes, the webpages and mobile applications of the company as the private holder of information must correspond to the requirements of section 32 of the

Public Information Act. For further information on this topic, see section 32 of the Public Information Act, directive No. 2016/2102 of the European Parliament and of the Council, as well as Commission implementing regulation No. 2018/1523.

- **Clarify** whether the company needs to acquire a data protection officer. If a data protection officer is needed, then ensure that the person is sufficiently competent. In addition, make sure that all necessary information security know-how is available (among your staff or externally).

Recommendations to a head of a public authority

- **Acquire a competent** data protection officer and ensure that the authority has an information security manager (among your staff or externally).
- **Implement** relevant and necessary security measures to protect personal data.
- **Establish** and implement internal control mechanisms in order to discover the violation of the requirements of personal data processing as well as violations of the requirements of processing data for internal use in your authority.
- **Map, create, update.** The following is necessary:
    - a balance-style data processing register, which would first and foremost give an overview of processed personal data and the legal basis for their processing;
    - risk assessment for taking security measures pursuant to the Cyber Security Act;
    - an overview of information assets pursuant to section 12 of the "Principles for Managing Services and Governing Information" regulation;
    - document classification scheme according to the "Archive rules".
- **Make sure** that the requirements of data processing directed for the public as well as officials are updated, that means sufficiently clear, simple, and

understandably worded. Ensure that the requirements of data processing are easily found on the authority's webpage.

- **Be prepared** for situations where a data subject wishes to see his/her personal data, requests that they be amended, deleted, their processing restricted, or wishes to give objections. If you amend, delete or restrict the processing of personal data, then be prepared to notify those recipients who have received personal data from the authority.

- When forwarding data to third countries, **clarify** whether there is a suitable legal framework for this – for example, there is a decision of the European Commission about the sufficient level of data protection, when to use appropriate safeguards or when the personal data are forwarded according to derogations for specific situations. Considering the current situation, this has to be also clarified in a situation, where personal data are forwarded to the United Kingdom – especially in the case of no-deal Brexit.

- **Make clear early** in which violations of personal data processing you are required to contact the Estonian Data Protection Inspectorate within 72 hours. In some situations, the data subjects and the Information System Authority of Estonia have to be notified.

- **Before you begin** a new type of personal data processing for the authority, conduct a written data protection impact assessment. If this new type of personal data processing is related to a situation where, due to changes in legal acts, the authority is given additional rights or possibilities for processing personal data, check whether the explanatory memorandum of the draft legislation includes a data protection impact assessment. If the explanatory memorandum of the draft legislation has no such analysis or if it does not cover all planned personal data processing activities, conduct a data protection impact assessment.

- **Conduct** a written open data impact assessment (see section 3^1 of the Public Information Act).

- **Check** whether the establishment has created a legal person governed by private law or given public functions to it, and if yes, then help the company to clarify to what extent the requirements of the Public Information Act are governing it.

- **Ensure** that the data of databases entered into the administration system of the state information system is updated and has received necessary approvals.
- **Make sure** that the webpages as well as mobile applications of the authority are accessible. For further information on this topic, see section 32 of the Public Information Act, directive No. 2016/2102 of the European Parliament and of the Council, as well as Commission implementing regulation No. 2018/1523.
- **Train** officials, give explanations and (written) guidelines which help to legally process personal data on behalf of the authority.
- **Check** that the officials have knowledge about document management and classification of information as internal – training has to be done for that.
- **Take responsibility.** Persons responsible for the document management of an authority should check the external view of the establishment's document register to check for possible errors and violations.

Recommendations to lawmakers and preparers

The following recommendations are meant for those who create, draft, prepare or give input to legal acts which are related to the fields of activities of the Inspectorate.

- Before regulating the possibility of processing a new type of personal data or amending an existing one, ensure that it is actually needed. Do not act hastily or without considering all circumstances.
  Apply principle – measure nine times and cut once.
- As one part of the explanatory memorandum of the draft law, prepare a data protection impact assessment. For that, see chapter 5 of the Inspectorate's general guidelines for controllers and processors and annex 1 of the general guidelines.
- I recommend to analyse in the explanatory memorandum of the draft the constitutionality of personal data processing or in other words, whether it corresponds to section 26 of the Constitution of the Republic of Estonia.
- When amending a legal act, ensure that the existing legal framework or planned amendments also provide legal protection to the data subject. For

example, so that authorities would not receive a right to mass-process the personal data of a data subject indiscriminately without the knowledge of the data subject – in this case, the data subject cannot exercise legal remedies to protect his/her rights. If the legislation includes an exception in regard to not notifying, then it has to be proportional and necessary.

- When you amend the statutes of some database, conduct an impact assessment on the open data of that database, if it has not been conducted already.
- As a separate note, I recommend to the Ministry of Justice to establish the possibility of an administrative fine in the Estonian legal system, because sanctioning legal persons via current misdemeanour proceeding is inefficient and encumbers all parties.

Acknowledgements

2018 was a very stressful year which was characterised by constantly adapting to changes. The data protection laws were updated and the Inspectorate moved into a new location at Tatari 39 at the end of the year.

I would like to thank my former as well as current colleagues in the Data Protection Inspectorate who were part of the process, and helped to conduct all activities in 2018. And for this I am truly grateful to all of you!

In addition, I would like to thank the members of the Public Information Council, who have helped to pass on the skills and knowledge in regard to data protection and handling public information in their domain. I would like to thank colleagues from ministries, authorities, local governments and partner organisations.

Raavo Palu

Legal Director

In the capacity of Director General of the Estonian Data Protection Inspectorate