Annual Report 2016

SUMMARY and RECOMMENDATIONS FROM THE DIRECTOR GENERAL
This year and the next year the Estonian Data Protection Inspectorate will be focussing mainly on ensuring a smooth implementation, appropriate in Estonian circumstances, of the new data protection rules.

### Data protection rules are renewed

As from 25/05/2018, the General Data Protection Regulation 2016/679 will be applied. The Data Protection Directive 95/46 of 1995 and the Personal Data Protection Act will become invalid. Although the regulation is directly applicable, it does leave some manoeuvring space for the legislators of the member states. This especially regarding data processing in public sector.

In addition, Directive 2016/680 must be adopted as regards data protection in penal law proceedings. The directive significantly duplicates the General Regulation. It was prepared as a separate act because the EU is not competent to establish norms for national penal law proceedings with a directly applicable regulation. The directive also establishes norms for penal law related data exchange between countries by replacing the relevant Council framework decision.

Implementation of the EU e-Privacy Regulation is also planned as from May 2018 (today it is only a Commission proposal). This would establish norms for the data protection special requirements regarding communication, and also direct marketing (spam, nuisance calls) instead of the e-Privacy Directive 2002/58 and Electronic Communications Act.

By May 2018, the new Network and Information Security Directive 2016/1148 which establishes norms for the electronic security of essential services of both private and public sector must also be implemented.

To execute these four items of related legislations (2 regulations and 2 directives), the Estonian parliament needs to pass implementation acts and amend a large number of current laws.

### New data protection rules – to what should the companies and agencies pay attention?

I would like to console the reader who feels overwhelmed by such an avalanche of acts and legislations: the foundation of data protection rules is still the same as before. All principles pursuant to the current data protection directive and laws valid in Estonia at the moment will remain valid.

True, a new and larger structure (legislation with new wording) is constructed on the old foundation (the principles valid thus far). The furniture of one house may not perfectly fit in another house. The same way, all information management systems, behaviours, contract forms, and document blanks used in the company or agency until now may not suit the new situation.

The common line of the General Regulation is risk based approach. The more sensitive the data processing, the more firmer the rules. A company or an agency that does not tackle sensitive data
processing and that has been following the rules until now does not need to make significant changes.

However, those who collect and use sensitive personal data and large databases, use automatic profiling or large scale camera surveillance should definitely check their work organisation, information systems, and document blanks.

The most significant substantial change in the entire private sector is the portability of personal data. A person can take their digital data from company A and transfer it to company B. Companies who will likely receive a large amount of such requests are wise to check their information system(s) so that transfer of data would be as efficient and simple as possible, their costs would be optimised, and customer satisfaction increased. It is also important to consider the requirement of generally used structured machine-readable format.

**New data protection rules - what does the Inspectorate do?**

The Inspectorate advises the Ministry of Justice and the Ministry of Economic Affairs and Communications in preparation of the implementation acts. I published the initial observations and recommendations in the overview of 14/10/2016.

Also, we are participating in related preparatory work within the framework of the Working Party of European Data Protection Authorities. On 25 May next year the Working Party will become the European Data Protection Board. Since the Board will, among other things, also solve disputes between member authorities, participation in the development of common perspectives is highly important.

I recognise my colleagues who work through the voluminous materials of the Working Party aside from their work at the Inspectorate and also contribute to these materials by e-mail and by participating in sub-groups in Brussels. If a small agency wants to be considered a partner among significantly larger agencies that have separate employees and units for this work, it leads to extensive effort. This work, however, is worth the effort. The data protection rules leave a lot of room for interpretation. This affects European and Estonian e-governance, digital economy, and information society. We want to be leaders not followers.

The General Regulation authorises the national Data Protection Authorities to determine several requirements which affect the obligations of companies and agencies. The Working Party has either covered these questions already or is about to cover them in the frame opinions.

The Inspectorate will publish the structure of the general guidelines of the General Regulation before Midsummer. We will gather all general guidance texts into one document. In this document, we will specify requirements for breach notifications, data processing register, data protection impact assessment, pre-consultation with a Data Protection Authorities, data protection officers, and data protection by design and by default. We will approve the general guidelines after discussion at the autumn meeting of the Advisory Council of the Inspectorate. Some clauses will remain open – these need to be approved by the future European Data Protection Board.

We will prepare an individual’s data protection rights leaflet. To help data controllers processing personal data, we will prepare a “check list” on how to obtain a proper consent for processing
Also, we will prepare sample documents concerning data protection conditions for companies and public sector agencies. We are ready to help business and professional associations if they want to develop sample documents for more specific areas or business fields.

During the first half of 2018 we will focus on checking the existing guidance texts.

As a trainer and advisor, we are not expected to be theoretical but to provide practical approaches for specific areas of life. As the majority of questions will be answered only during the process of developing the guidance texts, the volume of our training and advising activities is rather small. We will concentrate on creating the guidelines. As a by-product of analytical preparation work, we will publish a series of topical articles on our webpage.

In addition to creating the guidelines, we are also focussing on the qualification of the data protection officers. Renewal and expansion of the data protection rules and development of technology set the bar quite high. A previously gained diploma in law or IT may not mean that the person has (sufficient) data protection and information security knowledge and skills.

In preparing for the changes of 2018, both private and public sectors need a large number of specialists. The Inspectorate consulted with business and professional organisations and universities. As a result, on 21/12/2016, the description of the tasks, knowledge and skills of a data protection officer was created.

This base document was developed following the structure for professional standards and is mainly meant to serve as supporting reference material in updating the training programmes and curricula of universities. Upon their request, we have advised the universities regarding this. The Inspectorate is also prepared to host an optional basic knowledge examination in 2018 for data protection officers if such need should arise.

Policy recommendations for 2017 and 2018

The new data protection rules include quite significant specifications for private and public sector. Therefore, I will divide the main recommendations in two: recommendations for the entrepreneur and recommendations for the public sector bodies.

1) Recommendations for the entrepreneur – integrated assessment, portability, data protection officer

If processing of personal data is a large-scale process in your company or involves considerable risks, conduct an integrated assessment of your data processing. Observe your entire work order, information systems, and document blanks from the perspective of the new data protection rule. This way you will instantly get a wholesome result which

- includes data protection impact assessment (article 35 of the General Regulation) together with risk management;
- defines data processing register (article 30);
- implements data protection by design and data protection by default (article 25);
- implements the procedure of breach notification (article 33, 34) and
- documents the data protection conditions of the company for clients and partners (article 12-22 requirements).

Be sure to check the data portability (article 20) in your work processes and information systems. I forecast that this will be the costliest and most time consuming of the implementing activities. Portable information must be in a widely used machine-readable format and structure. Do not leave this to the last minute as this may be required already from the first day after the General Regulation enters into force.

Regardless of whether or not the General Regulation (article 37-39) requires you to determine a data protection officer, find a specialist to assist you. Do not trust dilettantes! Send your own employee to a trusted training course or make sure an external consultant has undergone relevant training. The specialist must be capable of connecting data protection and information security requirements with the actual work processes and information systems of your company. A theoretician who can merely recite laws will be of no use.

2) Recommendations for the public sector bodies – integrated assessment, connection to freedom of information, data protection officer

Conduct an integral assessment of data processing in your agency considering the General Regulation, Public Information Act (Freedom of Information Act) and the legal acts relevant specifically for your agency. Your work organisation, information systems, and document blanks must consider these. This way you will instantly get a wholesome result which

- includes data protection impact assessment (article 35 of the General Regulation) along with impact assessment of making information accessible as open data (subsection 31 (3) and clause 28 (1) 31²) of the Public Information Act, incl. consideration of setting so-called mass restrictions and licenses);
- defines data processing register (article 30);
- conforms current requirements of database maintenance to the General Regulation, updating what is entered regarding the database in the State Information System’s Administration System (Chapter 5¹ of the Public Information Act);
- covers the requirements of keeping a document register (sections 11 and 12 of the Public Information Act, incl. the requirement to present the data of physical persons anonymously in public view, valid as from 16/01/2016);
- implements data protection by design and data protection by default (article 25);
- implements the procedure of breach notification (article 33, 34) and
- documents the agency’s privacy policy (requirements of article 12 –22) which, pursuant to clause 28 (1) 31¹) of the Public Information Act, must be published on the agency’s webpage.

Public sector agencies that offer goods or services to clients who are physical persons based on civil law should apply data portability similarly to companies (article 20).

Appointing a data protection officer (article 37–39) is obligatory in all public sector agencies; regarding everything else, the recommendation is the same as for the companies.
Past and future views in more essential work flows

a) Statistics

I conclude last year’s work flows in following numbers:

<table>
<thead>
<tr>
<th>ACTIVITY INDICATORS</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>incl.2016 PDPA, ECA//PIA ¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of guidelines, policy advising</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a) guidelines (not considering updates to existing)</td>
<td>4</td>
<td>12</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>b) opinions on draft legislative acts (upon approval of a database, the database statutes are usually assessed; this is not presented here, see row ‘r’)</td>
<td>21</td>
<td>30</td>
<td>28</td>
<td>35</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Communication work</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) questions, memoranda, freedom-of-information requests</td>
<td>817</td>
<td>1370</td>
<td>1144</td>
<td>1369</td>
<td>1417</td>
<td>1136//281</td>
</tr>
<tr>
<td>d) help line calls</td>
<td>1160</td>
<td>1344</td>
<td>1141</td>
<td>1136</td>
<td>1419</td>
<td>1148//155</td>
</tr>
<tr>
<td>e) counselling (companies, agencies)</td>
<td>56</td>
<td>69</td>
<td>34</td>
<td>33</td>
<td>79</td>
<td>77//2</td>
</tr>
<tr>
<td>f) training events (organised or participated as a trainer)</td>
<td>18</td>
<td>19</td>
<td>24</td>
<td>18</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Supervision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g) circulars (without opening supervisory cases)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>incl. No. of circular addressees</td>
<td>4</td>
<td>149</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h) large-scale comparative monitoring sessions</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>14</td>
<td>9</td>
<td>6//3</td>
</tr>
<tr>
<td>incl. No. of objects observed</td>
<td>412</td>
<td>148</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i) complaints (submitted)</td>
<td>404</td>
<td>550</td>
<td>413</td>
<td>446</td>
<td>390</td>
<td>251//139</td>
</tr>
<tr>
<td>j) ex officio supervisory cases (open without complaints)</td>
<td>191</td>
<td>171</td>
<td>152</td>
<td>384</td>
<td>86</td>
<td>83//3</td>
</tr>
<tr>
<td>incl. preventive data protection audits</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>24</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>k) on-site inspections (in supervisory cases)</td>
<td>23</td>
<td>15</td>
<td>48</td>
<td>35</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>l) recommendations and proposals (in supervisory cases)</td>
<td>299</td>
<td>56</td>
<td></td>
<td>46//10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>m) precepts (usually preceded by a proposal; usually includes a coercive fine warning)</td>
<td>187</td>
<td>120</td>
<td>86</td>
<td>77</td>
<td>59</td>
<td>43//16</td>
</tr>
<tr>
<td>incl. regarding registrations (without previous proposal)</td>
<td>130</td>
<td>67</td>
<td>45</td>
<td>28</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>n) misdemeanour cases (closed)</td>
<td>43</td>
<td>29</td>
<td>11</td>
<td>16</td>
<td>16</td>
<td>16//0</td>
</tr>
<tr>
<td>o) penal law fines (for misdemeanours) and coercive fines (in supervisory cases)</td>
<td>39</td>
<td>22</td>
<td>8</td>
<td>15</td>
<td>16</td>
<td>16//0</td>
</tr>
</tbody>
</table>

¹ PDPA, ECA//PIA - Personal Data Protection Act, Electronic Communications Act // Public Information Act
The volume of communication and consultative work increased significantly last year: responses to questions and help line calls, individual consultations. As reasons, I mention increased awareness (that who doesn’t know will not ask) but also IT-development (new practical privacy issues cropping up). Questions regarding renewal of the data protection rules also stood out.

The volume of large-scale monitoring reduced during the past year. This decrease is mainly due to public sector supervision. In previous years, municipalities (more than 200) were in the focus of our monitoring sessions and post-monitoring follow-up cases. Due to the administrative reform, we directed our attention to state agencies last year which considerably decreased the number of supervised objects.

The unexpectedly substantial number of people leaving the agency (5 out of 18) also contributed to the decrease in supervision volume. Temporary vacancies and training of new colleagues take performance indicators down.

This year, we are planning to considerably increase the volume of on-site inspections (last year 33; this year 55 are planned).

b) Public sector information – wholesome supervision over information management

In addition to protection of personal data and access to public sector information (incl. access to open data), as from 16/01/2016 the Inspectorate also oversees, as requested by the lawmakers, the requirements of database maintenance and protection of restricted information (except classified information for national security purposes) in public sector bodies. This allows for an integrated approach in preventive supervisory work. We assess all the aspects of information management - ease of access to information and level of protection of restricted information.

Above is also monitored during annual monitoring of agencies’ online information – this is dubbed “traffic light monitoring”. Monitoring of public agencies last year was great because no one received a red light assessment. The Office of the Prosecutor General and Saare County Government won the titles of the most transparent agencies.
Last year, the number of challenges related to private holders of public sector information increased, due to both legal complexity (limiting information related to a public task of a private entity is always complicated) and low awareness of holders of information.

Malicious laziness in responding to requests for information is a point of concern. 1/3 of information requests were performed during challenge proceedings. Laziness is also visible in the tendency to explain the refusal of performance of request for information only as late as during appeal proceedings.

Two measures are planned to reduce these concerns. First, this year, we will conduct a larger number of on-site inspections – we will pre-emptively assess how well the work organisation and preparation of the employees in a specific agency enable adherence to requirements of the Public Information Act. The inspections will involve the organisation as a whole of information management at a company. Secondly, if a person is caught in an act like that, we will start using the right given to the Inspectorate to demand the initiation of disciplinary proceedings regarding this civil servant.

The situation at the time of taking over the supervision of the public sector databases (16/01/2016) can be summed up with two fractions: 1/3 of database keepers disregarded the requirement to approve and register the database in the Administration System of the State Information System and 2/3 disregarded the requirement for information security audit.

So as to bring database maintenance into order, we forwarded circulars to relevant agencies. In addition, we have a regular correspondence with the State Information System Authority (national IT and cyber security agency, in charge for the data exchange layer, or x-road, and information security system) and the Ministry of Economic Affairs and Communications (regarding agencies that apply for IT investments but whose databases, in our opinion, are not in order). As a result, a problematic database may be refused access to x-road services and they may not receive the investment money.

The number of databases registered in the Administrative System grew during the supervisory year from 353 to 492 (28%), incl. the number of those that gained approval for use, which grew from 208 to 277 (25%).

We agreed on the organisation plan and deadlines with the key ministries. As a result, the number of problematic registers decreased for the Ministry of Education and Research from 12 to 3, for the Ministry of Justice from 30 to 6, and for the Ministry of Social Affairs from 17 to 8. The Ministry of Environment promised to bring the databases under their management into order by the end of 2017 and the Ministry of the Interior promised to bring the databases with high security classes into order by the end of 2017 and rest by the end of 2018.

Unfortunately, this mainly concerns the problems reflected in the Administration System. Several databases are still seriously struggling with a more significant problem – data quality (especially e-health and the criminal records database).

Concerns regarding access to databases relate to the Business Register (availability of the contact information of erased sole traders), the Land Register (free of charge ownership inquiries made by contractual clients) and the Marriage Settlements Register (publicity regimen of a paper filing system is unsuitable for the digital age).
c) information technology and privacy

More and more IT devices and software solutions enter the market. On the one hand, the intelligent demand of the clients is what influences the device manufacturers, software developers, and information system managers to have more respect for the client’s privacy. We try to support this both alone (series of articles on our webpage) and in collaboration with other parties (special thanks to the cooperation network Safe Internet Centre in Estonia and to the Information System Authority for the Andmejälgija (Data observer) project).

On the other hand, in the digital age, a person often goes from being a data subject to being a data object that cannot control even the information that is regarding themselves. The Inspectorate conducts comparative monitoring sessions concerning the use of technologies subject to privacy risks. Last year we observed Wi-Fi services in shopping centres. In sync with the Consumer Protection Board, we observed the mobile applications of online shops. The Inspectorate noted excessive agreement requests for accessing the device content, ambiguity of user conditions and shortness of information on exciting the service. In sync with the Data Protection Inspectorates of Latvia and Lithuania, we observed the level of protection of client data during warranty repairs of mobile phones and within the framework of global collaboration of privacy enforcement agencies (GPEN) we observed protection of personal data in smart home solutions.

We gave advice, among other things, also on cloud data processing and data embassies.

This year, we are planning to raise the data protection related awareness via start-up incubators, observe the e-education environments available in Estonia, prepare a guide regarding monitoring of smart devices in public space and a leaflet for installers and users of security cameras and other surveillance equipment. This year we have already published an explanatory guide for big data and privacy.

d) health and social protection

Data quality in health and social protection registers is still a significant concern. We expect the Centre of Health and Wellbeing Information Systems established on 01/01/2017 to change things.

In order to give clear and practical pointers to people without legal background in this legally complicated maze of problems, qualified lawyers should first digest these problems. If there is no base analysis, there is nothing on which to build relevant generalisations and guidelines. A voluminous guide Personal data in health and social protection sector, published last year before Christmas, is an example just like that. A guide that was initially planned as a practical material turned out to be a lawyer-to-lawyer analytical material.

Last year’s health audit series involved 24 first-level health facilities (general practitioners, occupational health doctors) – the same number as the year before. The results were, in general, satisfactory.

Last year we sentenced seven users of health data for a misdemeanour of unreasonable curiosity.
e) mass surveillance and legislative drafting

The general attitude towards bulk surveillance is negative. The European Court of Justice has expressed it repeatedly, incl. regarding surveillance of electronic communications networks. The general view is that if a majority of or the entire population is the object of constant data collection by authorities without any reason, fear will spread in the society. A person who knows that “Big Brother” can spy on them at any moment will not act naturally and can be manipulated. The massive data occurring as a result of mass surveillance is, in turn, a source of risk of potential malicious use.

However, on the same day with the data protection package the European Parliament also approved the Passenger Name Data Record Directive 2016/681. This allows law enforcement authorities to completely supervise the passengers’ booking information of all flights outside of the EU and if necessary also within the EU. At the same time, it is a balanced process – everyone’s data is “run through the machine” but only information related with terrorism and other serious criminal suspicions is maintained longer. A permanent super database of every person’s each flight is not created.

This can be compared to speed cameras. All cars pass the camera lens but the database only stores the information of those speeding and not everyone. The Ministry of the Interior came up with a similar idea, to “run through the machine” the data of all hotel guests, to find guests with terrorism and criminal suspicions.

Thus, mass surveillance can be allowed on some occasions. But the lines between normal and mass surveillance must be clarified better. Law enforcement, misdemeanour and criminal laws, as well as specific laws allow making single inquiries about a person. This both for investigating what has already happened and for prevention.

In the annual report of last year I disapproved the plan to give the Tax and Customs Board unlimited access to all databases, also the right to request communication data from telecom companies for risk evaluation (tax spying). This would allow constant automatic “scanning” of the data of all tax payers. Regrettably, this amendment to the Taxation Act was nevertheless approved in March this year.

But using the existing procedural provisions, worded considering single inquiries, for mass inquiries is also unacceptable. Making single inquiries does not mean combined data browsing in all databases.

I recommend limiting mass inquiries more specifically in legislation drafting to better balance the protection principle related rights and freedoms and security and protection of public order. This means that total preservation of communications data needs to be checked (it is conflicting with relevant European Court of Justice judgement).
About the Inspectorate

As before, our Inspectorate employs 18 people. We continue to be the only public sector body in the country where only civil servants work – all contractual support services are outsourced.

While in previous years our staff has been stable (number of people leaving is 1 or 0), last year 5 people left (incl. the first ever retirement in the Inspectorate).

In 2015, the Inspectorate’s budget was €671,725. Last year’s budget was €700,821. Almost all of the growth came from taking over the supervision of databases from the State Information System Authority. Our budget was increased by the cost of one position which we divided between the salaries of our existing staff. As the pressure on salaries was still prominent based on several colleagues’ leaving, we transferred €20,000 within the budget from economical costs to labour costs. This year’s budget is €700,482.

For six months already we have been the only state authority with no formal structure. Thus, we have no departments or first-level or middle managers. This allows increasing the number of people doing specific work and the flexibility of work organisation. Of course, this also means greater responsibility for the civil servants and more diversity in terms of the work content. For example, 8 out of 18 civil servants contribute to international cooperation and 5 to communication work. I am very grateful to all my colleagues thanks to whose commitment and professionalism all this has been possible.

We are aided by the Advisory Council who gives feedback to the agency’s priorities selection and contents of the guides. I recognise the members of the council who perform their social role with great interest and passion.

Viljar Peep
Director General, Estonian Data Protection Inspectorate

30/03/2017