The year through the eyes of the Director General

Looking back on and drawing inspiration from the previous yearbooks of the Data Protection Inspectorate, I noticed that for a few years already, the introduction has commenced with the realisation that the past year has been a year of changes. There is no denying that this foreword begins in quite a similar manner. Not so much due to 2019 having been a year of great changes, but more due to the fact that the moment and situation we are currently in is new and groundbreaking. It is likely that merely two months ago, I would have chosen a different beginning.

Today, I am writing these lines in a completely different world than it was two months ago – I am writing from home, from quarantine, while being part of a combat against a global pandemic. Quite a few people have said that the world will never return to what it was like before the COVID-19 virus and that in the future, we will be referring to the time before and after this devastating virus. Perhaps so.

What was the world like before the spring of 2020, i.e. in the year 2019, in terms of data protection?

The work of the Estonian Data Protection Inspectorate in 2019 was still affected by the entry into force of the General Data Protection Regulation. On the one hand, it may seem surprising that we are still referring to the GDPR as a new phenomenon. However, on the other hand, it must be admitted that the challenges of its implementation and I am afraid that also the joy of discoveries arising therefrom will continue for years to come. Let us also not forget that the domestic data protection legislation of Estonia was only updated in 2019 when the underlying Personal Data Protection Act was adopted.

However, the fact that the GDPR will remain a novel concept and offer new discoveries to the data protection authority certainly also stems from the small size of Estonia – we may experience various situations later than some of the large countries. Participation in the extremely active work of the European Data Protection Board has revealed that several interpretation and implementation challenges of the GDPR are, in fact, similar in nature, regardless of the size of the country. However, the position of a small country is certainly made more difficult by limited resources.

The Estonian data protection authority is practically the only such institution among the members of the European Data Protection Board that did not receive (and has still not received) additional resources to cope with the new tasks. We are also still one of the smallest state authorities in Estonia. At the same time, international cooperation alone has increased tremendously. The statistic figures of our activities are available on page 61 of this yearbook and these reveal that we received more than one thousand enquiries through the Common European Information System of Data Protection Authorities alone, a part of which also ended up as proceedings that reached the desktops of inspectors. The commencement of the one-stop shop cooperation of European data protection authorities for resolving cross-border cases has been discussed in more detail on page 19.

However, not only statistical figures are important. The substance of international cooperation is essential, as it generates the bulk of the knowledge on how to interpret or implement a certain provision or measure of the GDPR. This can be achieved by relying on the experience of other

authorities, actively participating in the preparation of guidance materials developed by the European Data Protection Board, as well as by participating in joint inspections.

Due to our limited resources, we must currently make very clear choices on where and how much we can contribute. We have rarely used the opportunity to offer to act as a rapporteur in guiding a certain topic in the Data Protection Board. Unfortunately, we have chosen to back out even in cases where the topic would have been interesting, as well as necessary for us: all due to the fact that acting as a rapporteur, i.e. a leader, in the Data Protection Board would require intensive work, which could only take place at the expense of other duties that require immediate action.

This leads us to another burning question that has been discussed as of the entry into force of the GDPR. Where are the fines? The statistics and content of the yearbook, as well as silence in the news indicate that we have not imposed any huge fines based on the GDPR. There have already been rumours from some of Estonia's neighbouring countries of the so-called first swallows in this area. Thus, we are receiving somewhat scared, but also judgmental and sometimes even condescending looks on our lack of fines. Even I am not a stranger to the legend that the inspectorate is unable, unwilling and incapable of imposing fines. This is partly true, but also partly false. On the one hand, as previously described, our resources are limited and the topics addressed, as well as the time and method of addressing them must be selected carefully. The same goes for fining. On the other hand, I have already said it several times and will repeat it here once more: I believe huge fines are not in line with the Estonian legal system, as these are rather intended as administrative fines, which our legal system does not recognise.

The sceptics can say what they want, but administrative proceedings are unsound and serve no purpose in data protection issues. Both due to the narrow rules, short limitation periods, as well as challenges regarding provision of evidence in the case of legal person responsibility, which are all inherent to sanction proceedings. Administrative proceedings are well suited, for instance, for the inspection of speeding and presence of fishing permits, and for imposing punishments in the event of violations, but not for fining a company for allowing possible extensive data leakage. No one expects the sad IT guy who pushed the button to be fined. The fine should be imposed on the organisation that let it happen due to its rules or lack thereof, as well as due to ill-thought and insecure processes. However, I am glad that we also reached a consensus in this issue with the Ministry of Justice and when life returns to a regular work rhythm, this ambitious plan, which had already been prepared for the implementation of the administrative fine, will once again be discussed and put into work.

It should be noted, that all of this was not meant to indicate to those who are awaiting a fine that we will sit quietly and wait for the regulation on the administrative fine. Not at all! In addition to fines, we also have a great option to use the instrument of penalty payment as a sanction. The imposition of a penalty payment also has another bonus – it can be done repeatedly and it is intended to influence the data controller to fix the problem. This is the direction we find important – guidance toward lawful behaviour, making data controllers aware why it is important to protect people's privacy.

Wide range of topics

The one common theme and keyword of 2020 will certainly be monitoring equipment, especially video monitoring equipment. The European Data Protection Board also completed a corresponding guide last year, the adoption of which in Estonia is one of our goals in 2020.

Here too, however, the changing of people's mindset is more important than fines. In order for openness and transparency to become the new norm in video monitoring as well. Although, there are signs in public spaces that indicate the existence of cameras, these rarely provide information on who the camera monitoring us belongs to and who processes these data. There is a clear need for a developmental leap in this area.

Being a travel enthusiast myself, it recently caught my eye that in Germany, there is a sign on the door or partition of each store of the shopping centre regarding the owner of the camera and the reason for monitoring. Although the sign included a fair amount of information, its size was of no competition to the name of the store and neither did it disrupt the view, as is generally believed in Estonia. That if all of this information were to be put onto a sign, no one can see in or out of the shop window or door. This is not true. It is a question of willingness and there are plenty of examples to take after.

Several poignant data protection related issues have recently emerged in the area of information technology – for instance, the use of mobile telephony data by the state, as well as research developers, development of mobile applications based on health data, remote communication and the e-solutions used therefor – either in the area of studying, e-medicine or remote work. All these topics are on the one hand very technical, but on the other hand very clearly and intensely related to the processing and privacy of personal data. We have marked the processing of data in research carried out via IT resources and the use of information systems and e-environments in institutions engaged in the area of medicine and education as our most important keywords for 2020. Even when offering the best solutions to the society, it must still be kept in mind that without carefully considering the aspect of data protection, such a solution is defective and a great idea may, in fact, become a breeding ground for problems. First, the state as one of the biggest if not the biggest data controller must acknowledge its responsibility and set a good example. It is definitely not great to implement legislation amendments in a rushed and reckless manner and, even more importantly, without discussion under the auspices that, for instance, "rapid times require rapid decisions", while knowing completely well that no one will remember to return to temporary provisions once the "rapid times" have passed to think through and discuss the provisions in detail. Thus, it may happen that people not only feel that there is an attempt to implement amendments in the shadow of the crisis, which infringe their privacy and will continue to affect their lives after the crisis, it may actually happen.

The case is similar for innovation and IT developments as well. Both are extremely necessary in an e-state. I personally and I believe most Estonians are rather open towards any new solutions that make life easier, including artificial intelligence. Quite a few of us would take a step further to simplify the organisation of everyday life and would welcome face recognition technologies, if it helped to save time, but we all want to be certain that the provision of such services would not include unseen data processing processes that undermine privacy. This also goes for the relationship with the state. The development of the e-state is very important and welcomed. However, it must be kept in mind during the creation and development of any IT solutions that real personal data is not to be toyed with. Every development should be well thought through, secure and transparent.

In conclusion, I would like to thank my team. As mentioned, 2019 was not an easy year for the inspectorate. Competition on the labour market also damaged the workforce of the inspectorate. At the same time, it gave an opportunity to involve various new and active people in our activities, whose initial achievements we can already read about on the following pages, but who are already waiting for the new challenges of 2020 with a sparkle in their eyes. However,

each learning process leaves a mark – for instance, in performance. Thus, the plans for 2019 may have been more ambitious than actually achieved, especially in the area of monitoring. Nevertheless, it can be said that it was an active and educational year, and the inspectorate had to work on various remarkable projects in additional to its day-to-day work.

I would like to thank our cooperation partners and colleagues from ministries, establishments, local governments and partner organisations. I am also grateful to the members of the Public Information Council. And I also thank everyone who has contacted us in one way or another and thanks to whom it is easier for us to understand what we have achieved with our message, which advancements we can be proud of, as well as what we should focus on in the future.

Pille Lehis

Director General of the Estonian Data Protection Inspectorate