



ANDMEKAITSE INSPEKTSIOON

COMPLIANCE WITH THE PUBLIC INFORMATION ACT AND ENSURING THE PROTECTION OF PERSONAL DATA IN 2020



YEARBOOK OF THE DATA PROTECTION INSPECTORATE

Thank you for your contribution to the yearbook

Pille Lehis, Director General
Maris Juha, Supervisory Director
Urmo Parm, Technology Director
Maarja Kirss, Cooperation Director
Liisa Ojangu, Legal Director
Elve Adamson, Lawyer
Sirje Biin, Lawyer
Raiko Kaur, Lawyer
Mehis Lõhmus, Lawyer
Kadri Levand, Lawyer
Ingrid Lauringson, Lawyer
Sirgo Saar, Lawyer
Signe Kerge, Lawyer
Helve Juusu, Senior Clerk
Triin Kask, Assistant

Editor Signe Heiberg, PR Advisor
Layout and illustrations Kustas Budrikas
Original photos: pixabay.com
Print and volume Koopia Niini & Rauam

Data Protection Inspectorate 2021
Tatari 39, Tallinn

Table of Contents

4 KEYWORDS OF THE YEAR

- 6 Guide on the treatment of legitimate interests
- 9 The historic Schrems II judgement
- 10 The data protection aspect of Brexit
- 10 The keyword of awareness raising was 'a new way'

12 FROM THE DESK OF THE PRACTITIONERS

- 13 Interim review of the monitoring of economic information portals
- 15 Data processing may not continue in the event of an objection
- 17 A company had to remove debt data from their website
- 18 Retention of personal data for 10 years for the purpose of detecting new fraud
- 19 Data protection in employment relationships
- 21 Data protection during the coronavirus pandemic
- 26 Distance learning was difficult in terms of data protection
- 26 Why has the use of security cameras become a problem?
- 29 Electronic direct marketing and telephone sales continued to cause many complaints
- 30 More clarity was expected from the conduct of studies for policy development
- 30 Procedure for determining the right to carry out background checks: air carrier, airport, and the internal security service
- 31 Why has my health data been viewed?
- 32 The right of successors to receive health data
- 32 Why did buying prescriptions from e-pharmacies for another person have to be stopped?

35 COMPLIANCE WITH THE PUBLIC INFORMATION ACT

- 37 Challenge proceedings
- 38 Responding to requests for information
- 39 Monitoring local governments

40 CHALLENGES

42 LEGISLATIVE DRAFTING DEVELOPMENTS

- 43 Amendments to the statutes of the health information system
- 45 The drafts prepared by the ministry of the interior
- 48 Other drafts the inspectorate provided its opinion on
- 51 Databases processed in the administration system for the state information system
- 53 Databases of local governments

55 JUDICIAL PRACTICE

59 THE DATA PROTECTION INSPECTORATE AND CROSS-BORDER CO-OPERATION

61 ACTIVITIES IN NUMBERS

- 61 The number of violation reports increased
- 62 There were fewer calls to the hotline than last year
- 63 The number of data protection specialists is growing

64 STATISTICS OF THE YEAR

65 LOOKING AHEAD



KEYWORDS OF THE YEAR

The year **2020** did not bring major changes to data protection, but the issue of health data processing emerged, prompted by the coronavirus pandemic. The lawyers of the Inspectorate have picked out the most important issues of the coronavirus pandemic to include in the yearbook. The coronavirus pandemic also gave impetus to a number of legislative changes, on which the Inspectorate was asked for its opinion. In some cases, there was haste and thoughtlessness, but we need to understand the difficult situation we were all in at the time.

In addition, one of the most interesting topics is the interim review of the supervision of economic information portals, which has been going on for several years. From the point of view of the Inspectorate, this is definitely a remarkable issue, because it combines the freedom of speech of the society and the human right to privacy. However, the interim review is only one stop in the whole process, and work will continue in this direction so that the collection and disclosure of human data could be transparent and compliant.

In this yearbook, the Inspectorate deals with one hitherto relatively unknown right, which is to the right to object. It can be assumed that data protection will only become strong in society if people are aware of their rights. What are the feelings of the Estonian public sector towards protecting the privacy of people and making information available? Not too confident. However, the overall picture gets a little better every year. Last year, the Inspectorate monitored the websites and document registers of local governments, the results of which can be read in more detail on the website of the Inspectorate, but general observations on the issues of the entire public sector can also be found in the yearbook.

One of the major issues of last year was whether and when people have the right to access the internal documentation of an agency. The issue was raised due to the growing public interest in environmental issues and the intervention of the Inspectorate ended with the issuance of the minutes of a packaging committee of an agency to the person making the request for information. It also became clear from what point in time is the information not

at the planning stage anymore and has instead become a finished document, regardless of the data medium on which it is stored. In the digital age, when information is no longer limited to paper, it was necessary to create legal clarity for the right to public information on any other data medium, including information systems.

2020 was also very fruitful in terms of legislative drafting. The section 'Legislative drafting developments' covers the drafts for which the opinion of the Inspectorate was considered important and those which deserve attention in the opinion of the Inspectorate. As many of the drafts concern issues related to databases, we have also reviewed the database approval procedure in the administration system for the state information system. Regarding the draft laws and statutes concerning various databases, the desire of the state to collect more and more data stood out. The whole world is becoming more and more data-based – it is said that smart decisions should rely on data. Therefore, this desire of the state is not surprising, nor should it be seen as a warning. However, it is the duty of the Inspectorate to constantly give the reminder that in the heat of the moment, one has to ask how much data should they be collecting, for what purpose, and for how long. Data processors had to be reminded of these questions quite often last year.

Although the court proceedings were more modest in 2020 in terms of their effective decisions, new knowledge emerged or old knowledge was confirmed. However, a number of important issues for the Inspectorate are still pending so we have to wait to obtain the views of our courts. Although court proceedings are often not a pleasant or quick way for the parties to reach solutions, they are sometimes an indispensable part of life to gain confidence in certain important issues. Therefore, the Inspectorate is excited as it waits for further solutions.

2020 also marked a shocking event for Estonia as an e-state. We are used to seeing the state as a conscious data processor in whose hands our personal data can be trusted to receive services, but in 2020, the state itself fell victim to a cyber attack.

The fact that the attack also affected the Ministry of Economic Affairs and Communications, which ensures that e-Estonia is functional and secure, makes the situation even more surprising. The extent of the attack and the resulting damage must be clarified in the proceedings conducted by the Prosecutor's Office. Last year saw another significant case in which the positive coronavirus test results of nearly 10,000 people were leaked from the possession of an IT institution. The Data Protection Inspectorate must find out the data security of the controller and its compliance with the data protection rules and analyse whether the institution has done enough afterwards to ensure the protection of personal data.

As a small country, it is extremely important for Estonia that it has proper foundation for storing data. The foundation for data processing is established primarily on the basis of the principles stemming from the General Data Protection Regulation. One of these principles is security, and practice has shown that this cannot always be guaranteed, although it should. The purpose of the Inspectorate is to overcome this difficulty through proceedings and to ensure that such situations do not arise in the future. Both the public and private sectors must ensure the security of the processing of personal data, even when they are in a hurry to set up the information systems. Being in a hurry and not paying enough attention to security often means that there will be data leaks.

A lot of the attacks are made possible by inadequate data security or non-compliance with data protection rules. The year 2020 confirmed that there is still some way to go before we can call Estonia a secure e-society, and the sooner we want to get there, the more aware we need to become of data protection.

As each yearbook should reflect a summary of the topics of most concern, this book will cover all the topics that were most relevant to people. Some of these topics have been covered in several previous yearbooks, but as data protection is so rich in nuances, each year is different.



Pille Lehis

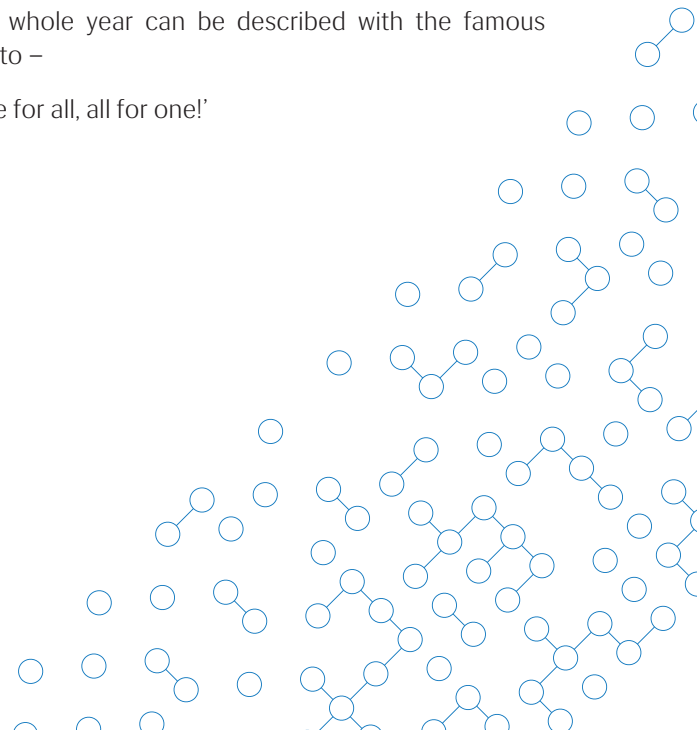
Director General

Special thanks go to the small staff of the Inspectorate who have done selfless work during this difficult time.

Many thanks to everyone who has contacted us. We thank our partners and colleagues, as well as contributors from ministries, agencies, local governments, and partner organisations.

The whole year can be described with the famous motto –

‘One for all, all for one!’



GUIDE ON THE TREATMENT OF LEGITIMATE INTERESTS

The advent of the General Data Protection Regulation (GDPR) brought one important change to Estonian data protection law – the right to process personal data on the basis of legitimate interest. Although provided for in the previous EU Data Protection Directive (95/46), it had not been transposed into the Personal Data Protection Act until the beginning of 2019.

Namely, Article 6 (1) (f) of the GDPR provides that the processing of personal data is lawful if the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Application of the guide on legitimate interests in practice

Unlike many other legal bases for the processing of personal data, relying on this legal basis requires a regular, three-step analysis. The European Data Protection Board, acting under the GDPR, has put the preparation of a guide on this issue on its agenda, but there has been little progress. However, Opinion 06/2014 on the notion of legitimate interest, drawn up in 2014 by the transnational Data Protection Working Party of the predecessor to the European Data Protection Board, which operated under Article 29 of Directive 95/46, can be consulted. This is because the wording of the provision on the legitimate interest of the GDPR has changed slightly compared to the Directive, but the nature and logic of application have remained the same.

‘Unlike many other legal bases for the processing of personal data, relying on this basis requires a regular, three-step analysis.’

Based on the aforementioned opinion of 2014 and taking into account Estonian practice, the Inspectorate prepared a guide in the spring of 2020 that explains how to implement legitimate interest as a legal basis for data processing.

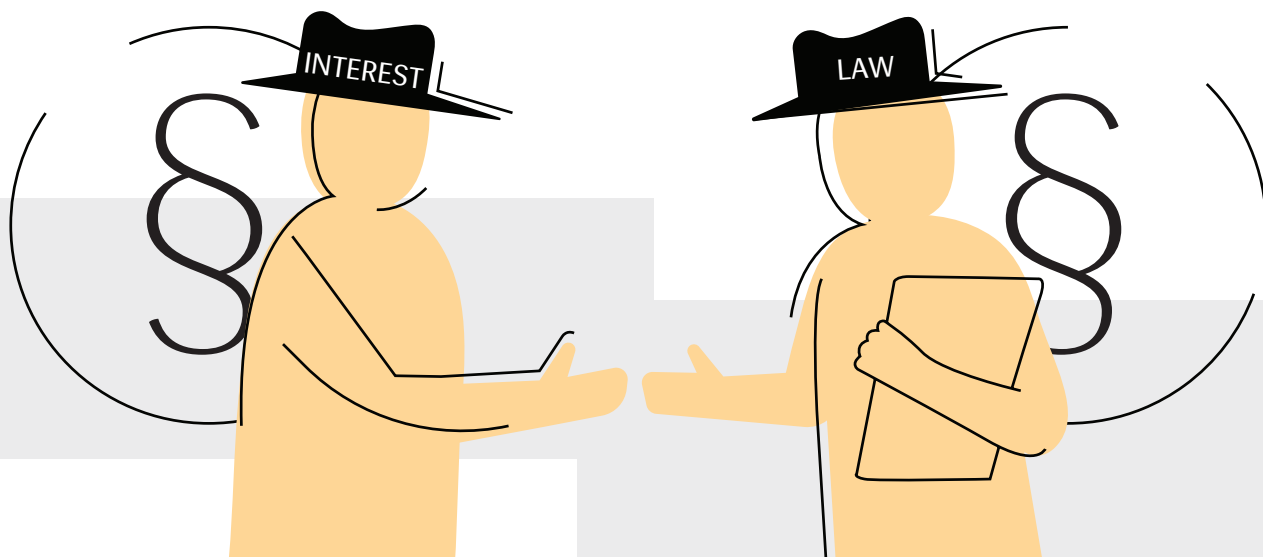
In short, the assessment of a legitimate interest takes place in three stages:

- I define what the interests of each party (the data processor, a third party, or the public) are, for which the processing of personal data is required;
- II define how and which data subjects will be affected by the processing;
- III consider the interests of each party and find additional compensatory measures if necessary.

In the private sector, a significant part of data processing takes place on this basis. Legitimate interest can be a legal basis, for example, for profiling customers of an online store when displaying an advertisement to them. It can also be a legal basis for storing customer data and purchase data for later legal disputes, using security cameras (both as a service provider and employer), and before concluding a contract, for example, when checking the solvency of a person. People have gotten the impression, largely as a result of media coverage of the GDPR, that it gives them full control over their data, as well as the right to demand that data processing be stopped at any time. The GDPR does provide such a right, but with many restrictions.

The companies themselves have certainly played a role in creating misunderstandings as their contract terms often included, among other things, the statement that ‘By signing the contract, the customer consents to the processing of their data for such and such purposes’. It is only when a person wants to withdraw their consent that it becomes clear that the company cannot stop processing the data because they need to keep performing a contract or be able to defend themselves against claims in court. Many people thus discover with great surprise that the company can process their personal data for many years after the transaction, even if it was a one-time purchase from an e-store.

Complicating matters further is the fact that the different legal bases for data processing – performance of the contract, consent, and legitimate interest – can all coexist in a relationship with the same data subject. In the context of data protection, they must be distinguished by data set, clearly indicating which data are processed on which legal basis.



Last year, the Inspectorate received several cases where a lawyer of a data processor sincerely referred to the invalid Personal Data Protection Act in a matter concerning security cameras. The use of security cameras was based on a special provision of the Personal Data Protection Act that was in force until the beginning of 2019. However, this provision no longer exists. It is also clear that the analysis of legitimate interests poses serious difficulties even for large companies. Unfortunately, attitudes probably also play a role in this. It is very common that companies start using legal aid services only after the Inspectorate has sent a precept or a demand for a penalty payment. In addition, the legal aid costs spent arguing with the Inspectorate could have been spent earlier on creating and documenting high-quality data protection rules.

Data processing of portals

An example is the economic information portals that have been operating in Estonia for many years, whose activities are based on legitimate interest. Although the Inspectorate compiled a thorough legal analysis of the activities of all information portals (web library of (www.aki.ee), on the basis of which it should have been easy for each information portal to put its documentation in order, the portals have not yet been able to do so.

There is a common misconception that data on all transactions (and the people involved) can be kept for 10–15 years to protect legal requirements. The General Part of the Civil Code Act does provide for a 10-year limitation period for claims, but only in the case of intentional breach of obligations. This means that if a company wants to keep personal data for 10

years for this reason, it must be prepared to show that there is a reason for it (that it really has a claim against the customer and that the obligations were intentionally breached). Legitimate interest arises from the rules of application that the justification for the processing (storage) of data must be specific and real, not merely hypothetical and speculative.

‘The most common thing the Inspectorate has had to deal with is errors in data collection. Namely, it is believed that everything that can be found on the Internet is also freely usable.’

The most common thing the Inspectorate has had to deal with is errors in data collection. Namely, it is believed that everything that can be found on the Internet is also freely usable. On the contrary, any processing of personal data that is not carried out for purely personal purposes must have a legal basis. The Supreme Court has also confirmed years ago that there must be a legal basis for the new use of personal data once disclosed. Therefore, the contact details of people cannot be collected from the Internet (including the commercial register, advertisement portals, or social media) to advertise goods to them (or make an offer to buy a forest). This is mainly due to the fact that the person has disclosed their telephone number or email address for other purposes. Commercial communications (which includes an offer to purchase a forest) may not be sent to the email address at all without the consent of the person or prior customer relationship.

‘On the contrary, any processing of personal data that is not carried out for purely personal purposes must have a legal basis.’

A separate area of concern is the disclosure of personal data on portals and social media groups (especially people warning other people of debtors). In this case, the person disclosing the information should first carry out an assessment of the legitimate interest (as there is no other legal basis). It should be noted that publication for journalistic purposes (and the relevant provision in the Personal Data Protection Act) is also based on the provision of legitimate interest of the GDPR.

In the case of processing based on a legitimate interest, the data subject has the right to object to the controller at any time due to their specific situation. Unfortunately, it appears that the data processors are completely unfamiliar with their obligation to respond to the request of the data subject. In many cases, the person has received an answer to their questions from the data processor only after contacting the Inspectorate. The data processors usually justify this with claiming that the letter was sent to the junk folder or their employee was inattentive. This is particularly the case when the data subject asks where the company got their data. Furthermore, some press publications still believe that they are not subject to the obligation to examine the objections of the data subject.

In the case of processing based on a legitimate interest, the data subject has the right to object to the data processor at any time, depending on their particular situation.’

As can be seen from the above, the need to assess the legitimacy pervades all areas and affects almost all data processors – from homeowners filming a street with a security camera to businesses living off data sales.

However, there is one big exception. It follows from the last sentence of Article 6 (1) and recital 49 of the GDPR that the public sector cannot rely on legitimate interest in carrying out its core tasks, but in non-core administrative activities, such as management of an agency or security of the building and information systems, legitimate interest could also be considered as a basis for data processing.

In conclusion, it can be said that data processors still have a long way to go before they can properly assess legitimate interest, but hopefully the guide of the Inspectorate and the developed practice will contribute to this.

discretionary decision relevance transparency
proportionality freedoms comparison of rights
data minimisation legitimate interest possibility of infringement
privacy interests purpose limitation
analysis person versus data processor

THE HISTORIC SCHREMS II JUDGEMENT

In July 2020, the European Court of Justice delivered a historic ruling annulling the Privacy Shield programme, but what did it entail?

The United States is considered a country with an insufficient level of data protection. Therefore, the conditions set out in Chapter 5 of the GDPR must apply to the transfer of data to the US. However, an exception was made – when the data was transferred using the Privacy Shield programme (a US-based company joined the programme and provided an equivalent level of data protection to the European Union), the transfer was considered to be of a sufficient level and the data processor did not have to apply Chapter 5.

The Safe Harbour programme, a predecessor of the Privacy Shield, was revoked by a court ruling in 2016 in what is known as the Schrems I judgement. In both cases, the plaintiff was Max Schrems, a data protection lawyer.

There was one noteworthy factor in the Schrems II judgment – the Court also pointed out that other additional safeguards for the transfer of data (listed in Article 46 of the GDPR) must assess whether the transfer ensures an adequate level of data protection and the rights of the data subject. This means that, for example, using standard data protection clauses for the transfer of data, which is also the most widely used safeguard for the transfer of data, it is necessary to assess their adequacy on a case-by-case basis. If necessary, additional safeguards must be put in place and, if this is not possible, the data may not be transferred.

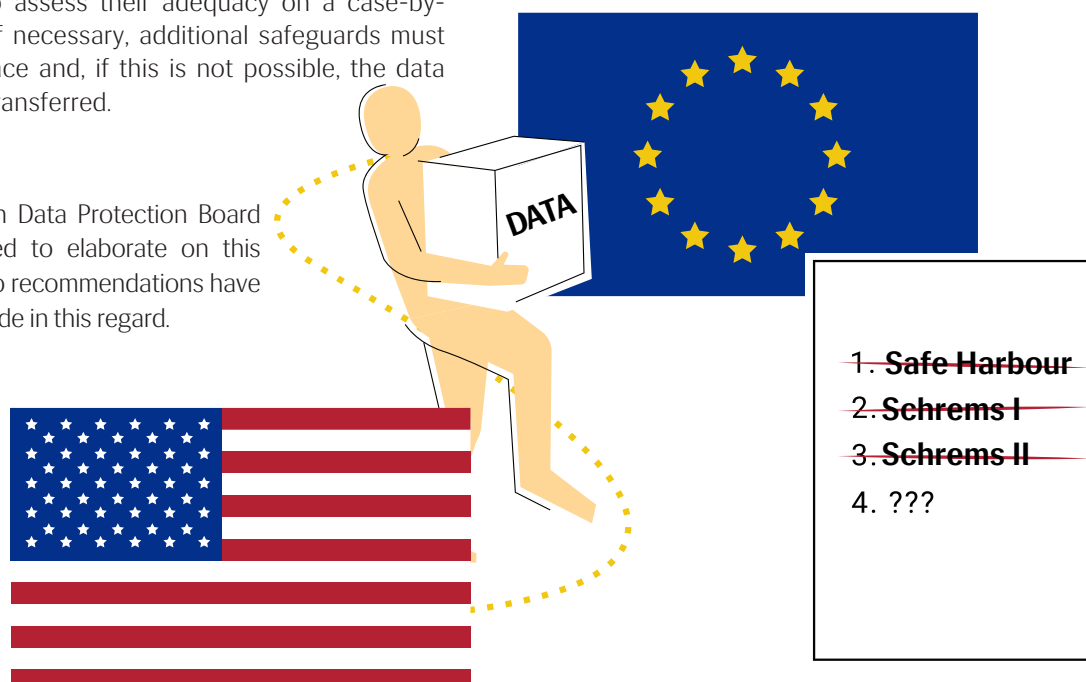
The European Data Protection Board was instructed to elaborate on this issue, and two recommendations have now been made in this regard.

Following the Schrems II judgement, the following documents were issued

I 'Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' the document is available on the website of the European Data Protection Board

II 'Recommendations on the European Essential Guarantees for surveillance measures' the document is available on the website of the European Data Protection Board

The European Commission started drafting new, improved standard data protection clauses which should take into account both the circumstances set out in the judgment and the recommendations of the European Data Protection Board. However, it cannot yet be said that this issue has been solved by the time the yearbook is published, and it certainly cannot be said that these guidelines and the new data protection clauses have solved the problem of transferring data to the United States. In the meantime, the Inspectorate recommends that data processors with US-based partners (controllers or processors) critically assess the need for data transfer and, if it is absolutely necessary, apply the provisions of the above recommendations.



The data protection aspect of Brexit

As the United Kingdom (UK) left the European Union, it will become a country with an insufficient level of data protection unless a decision on adequacy is taken for the UK by 30 June this year. Until 30 June, the data transfer will take place as before, i.e. the UK will be considered a country with an adequate level of data protection and Chapter 5 of the GDPR will not need to be applied.

Immediately after leaving the European Union, the UK started to apply to the European Commission for this adequacy decision, but this is a very time-consuming procedure. In some of the previous cases, this has taken years.

Therefore, until the UK receives adequacy status, it will be a country with an insufficient level of data protection and transfers of data to there are subject to additional safeguards under Articles 46 and 47 of the GDPR or exceptions listed in Article 49. This means an increased burden on the data processor, for example in the form of additional contracts (standard data protection clauses) or the creation of binding corporate rules (Article 47).

The latest news on this subject can be found on the website of the European Data Protection Board.

THE KEYWORD OF AWARENESS RAISING WAS 'A NEW WAY'

In the future, data protection will probably not be an issue for lawyers, IT professionals, and a few individual enthusiasts which is rarely discussed in the general public as most people are not interested in it. The digital life that absorbs data on a daily basis inevitably means that people have to understand the importance of effective data protection because without it, it is not possible to know who is doing what with the personal data, where, how, and with whom are they sharing it.

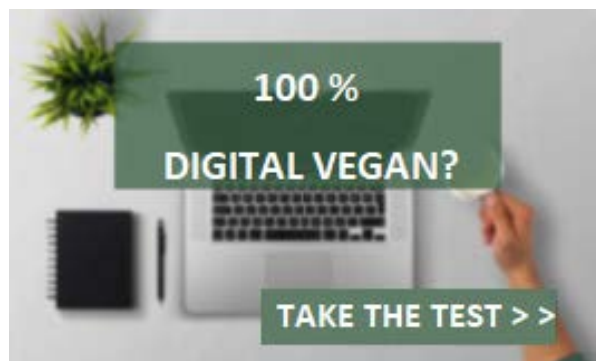
The Inspectorate has always considered it important to contribute to awareness-raising training, counselling, and the creation of guides. We did all of this last year to the extent that our resources allowed us. In addition to the usual information activities, the Inspectorate added new opportunities that would help to raise awareness of various target groups.

Knowledge tests

In order to explain the principles of data protection and to prepare for finding the right answers for oneself, the Inspectorate conducted 2 online tests last year: 'Andmekaitse ja raketiteadus?' (Data protection and rocket science?) and 'Digivegan' (Digital vegan).

The aim of the 'Digivegan' test was to give the test-takers the opportunity to find out whether they are environmentally conscious in terms of the

digital life in their everyday computer activities. Whether a person is careful with their personal data, i.e. does not share them with just anyone, is an important part of data protection. The test 'Andmekaitse ja raketiteadus?' allowed people to



Data protection and rocket science?

For raising awareness
among people.
TAKE THE TEST



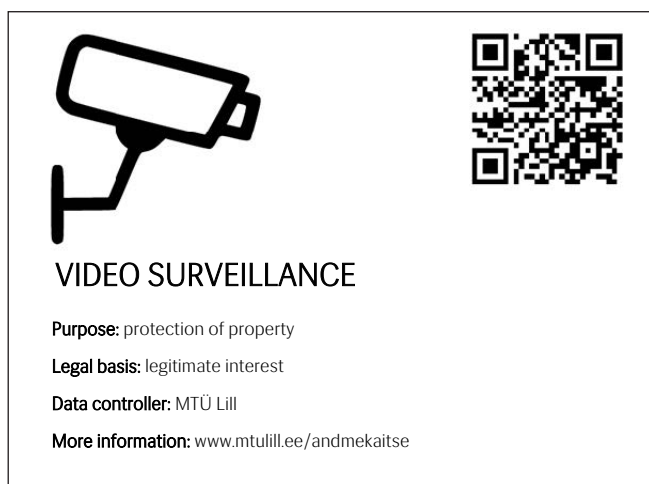
test their basic knowledge of data protection principles. Once a person has made the principles clear, they will be able to find the right answers in any situation with less effort. After all, no service can function without the use of personal data, and there are practically no areas that are not covered by data protection.

IT-based tool for getting a ‘Video surveillance’ sign

Last year, the Inspectorate, in cooperation with the Centre of Registers and Information Systems, also created a video surveillance sign generator, which helps the video surveillance organiser to obtain a proper notification sign file either for printing or sending to a printing house.

One of the biggest mistakes for video surveillance organisers has been missing or insufficient information. This, in turn, has led to many problems with both employees and between neighbours.

By creating a video surveillance sign with the generator, the person is also explained why it is important to add the required information to the sign and what it should look like exactly.



The easiest solution is to use the video surveillance sign generator on the website of the Data Protection Inspectorate – videovalvesilt.aki.ee.

New video seminars

In previous years, the Inspectorate has organised trainings, seminars, and conferences on the topics of the Personal Data Protection Act and the Public Information Act. Last year, however, the Data Protection Inspectorate started a series of video seminars. The added value of video seminars is that they can be watched at any time and as many times as needed.

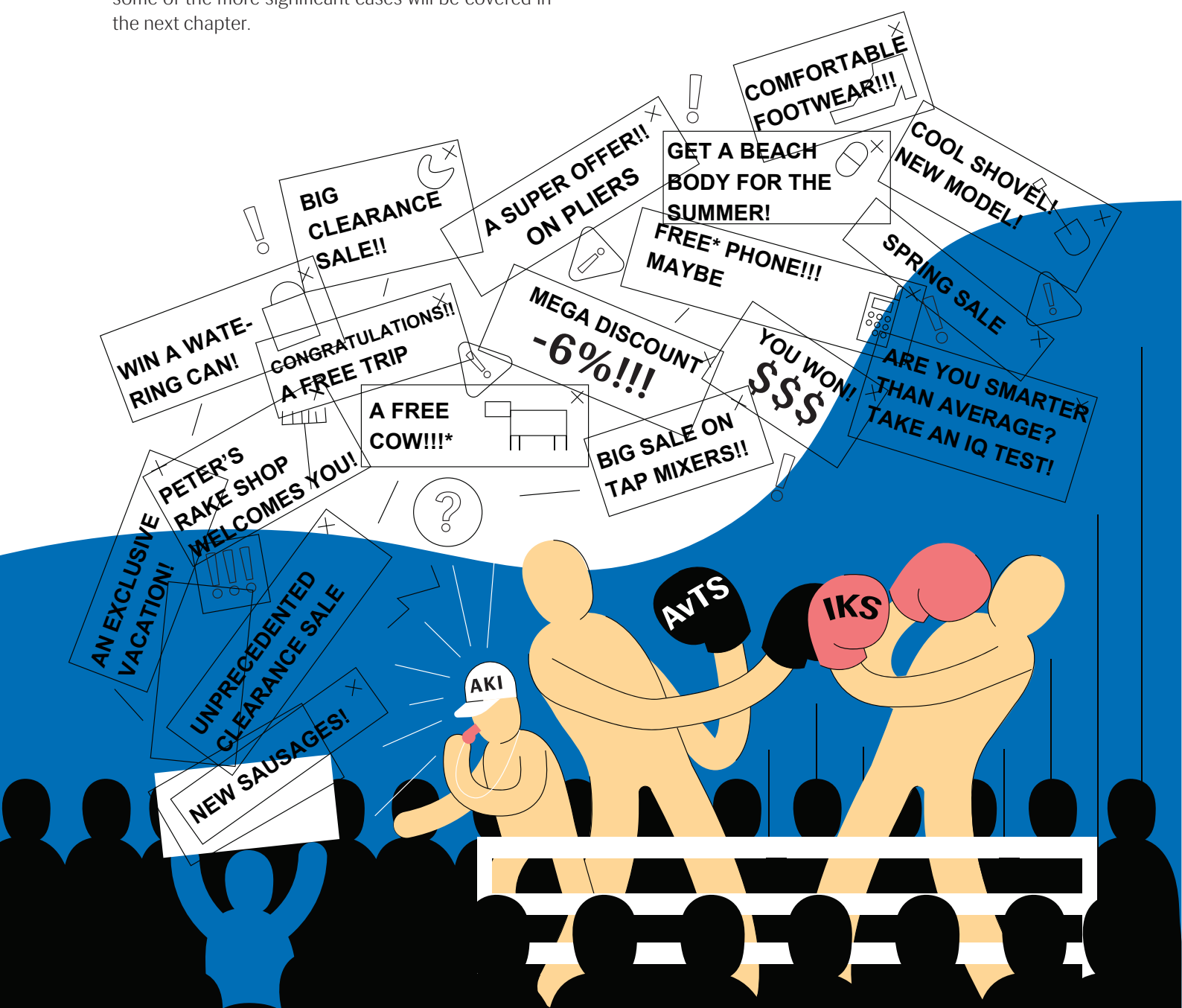
The first web-streamed video seminar was aimed at employees of educational institutions and explained data protection issues in distance learning and document management. The participants of the video seminar could ask questions both before and during the seminar.

The tests created, the video surveillance sign generator, and the video seminar diversified the information activities of the Inspectorate, and as they say, every little thing matters.

FROM THE DESK OF THE PRACTITIONERS

In 2020, our lawyers received about 150% more statements of claim and 25% more complaints.

The number of infringement notifications also increased by almost 20%. However, the number of requests for explanation and memoranda decreased by almost 35%. All in all, it was a very busy year and some of the more significant cases will be covered in the next chapter.



INTERIM REVIEW OF THE MONITORING OF ECONOMIC INFORMATION PORTALS



Over the years, the Inspectorate has received hundreds of inquiries from people who have found links to economic information portals (information portals) from Internet search results which have disclosed their personal data.

The Inspectorate initiated supervision proceedings over the activities of information portals in 2017, but with the entry into force of the GDPR in 2018, the legal order changed and this meant that the previous progress had to be reviewed in accordance with the new data protection law.

On 1 June 2020, the Inspectorate sent to the economic information portals (hereinafter information portal) a legal analysis and proposals for bringing its activities in line with the requirements of the GDPR.

The Inspectorate found that the operation of information portals is necessary, but the collection and disclosure of human data must be correct and the data processing transparent. The data processing of information portals must comply with data protection rules and principles.

Views of the Inspectorate

The processing of personal data concerning a natural person (including court decisions, official announcements, media coverage) in information portals is permitted only to the extent that fully complies with section 10 of the Personal Data Protection Act and Article 5 (1) of the GDPR. For example, it is prohibited to process (collect, compile, transmit):

- a) biographical data (e.g. place of birth, mother tongue, educational background);
- b) data related to party affiliation;
- c) data related to registered immovables;
- d) persona stories that give people a negative or suspicious impression and are often not related to a specific person;
- e) scores if there is no transparency in their formation.

Data protection conditions that fully comply with the requirements set out in Articles 12–14 of the GDPR must be established and published on the website.

A document must be prepared describing the existence of legitimate interest in sufficient detail (analysis/assessment).

The information portals are obliged to ensure that the data subject has the opportunity to submit an objection, as well as resolve the objection based on the content of the objection. In a situation where the request of the data subject is not granted, the information portal must prove that there is a valid legal justification for further processing.

Additional safeguards need to be put in place, such as greater transparency for data subjects and the creation of an electronic environment that allows them to see and use their data and object to its processing.

All the views of the Inspectorate can be found in the online library under the 'Teavitus, juhised' of the Estonian website of the Data Protection Inspectorate at www.aki.ee.

Although information portals published information taken from the commercial register, this was often done in conjunction with additional data about the person that they had successfully obtained from other sources. For example, data from the commercial register were related to official announcements, court judgments, newspaper articles, real estate, debt information, ratings, party affiliation, and even CVs. The information collected from various public sources was often open to search engines, but it bothered many people.

Considering that if the tasks of information portals are to ensure the verification of the right of representation and reliability of a legal person as well as the checking of creditworthiness of a natural person, it is necessary to perform data processing operations. In doing so, the principles of purpose limitation and minimisation must be observed.

Since making the proposal, the Inspectorate has checked the compliance of each information portal with the data protection requirements, including the content of the proposal.

If the controller of the information portal has understood how to comply with the data protection requirements and, in the opinion of the Inspectorate, has theoretically brought its activities into compliance with the conditions provided by legislation, then the Inspectorate also considers it necessary to check the prepared documentation (data protection conditions, analysis of legitimate interests) and the actual scope and manner of data processing for all information on the website of a specific information portal. To this end, the Inspectorate requests access to personal data.

2017	Start of the supervision
2018	Data protection law changed on 25 May
2019	Supervision
2020	Interim report

‘As at the end of 2020, none of the monitored information portals fully complied with the legal requirements for data processing.’

However, it can be said that the information portals had largely agreed with the proposals of the Inspectorate and made corrections and changes to bring their activities in line with the legislation. Based on the inquiries received by the Inspectorate, it can be noted that information portals no longer fail to answer questions sent to them related to the processing of personal data. They have also responded to the objections of people to the processing of their data and removed personal data from their websites.

The supervision of information portals will continue in 2021. The Inspectorate also focuses on ensuring that the rights of the data subject are guaranteed in information portals, including that people can access their personal data. Upon receipt of the objections of the persons, the personal data must be deleted or the objection must be assessed and the compelling legitimate reason for continuing the processing must be specified (Article 21 (1) of the GDPR).

DATA PROCESSING MAY NOT CONTINUE IN THE EVENT OF AN OBJECTION

Article 21 (1) of the General Personal Data Regulation gives the data subject the right to object at any time to the processing of personal data concerning them which is based on legitimate interest, including profiling based on this provision.

Upon receipt of the objection, the controller may no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject or for the establishment, exercise, or defence of legal claims. The data subject has the right to object based on their specific circumstances and justify why they consider the processing of their personal data unreasonable. In that case, the controller must, on the basis of the objection, reassess the situation of the individual, take into account the content of the objection, and demonstrate that they have a valid legitimate reason to further process the data in the specific case.

Objections require a reply

Even if there is a valid legitimate reason for further processing of personal data, each data processor has an obligation to refer to the individual and their specific objections in the event of an objection, and the analysis of further processing must take all this into account. In the event of an objection, it is not permitted to simply refer to the initial assessment of the legitimate interest or to the data protection conditions.

If the controller is unable to prove to the person that, in the light of the situation of the objector, they can rely on a legitimate interest of themselves and/or a third party and there is a valid legitimate reason to process the data, further processing of the data is prohibited in this respect and the processing of the data must be terminated and the data deleted (Article 17 (1) (c) of the GDPR). In addition, as a result of resolving the objection, it may be necessary, for example, to change the scope of data processing, i.e. instead of disclosure, the data will only be transferred to specific third parties pursuant to the conditions provided for in section 10 of the Personal Data Protection Act.

The possibility to file an objection is created for a person to be able to point out situations that the data processor could not have thought of earlier. The fact that the data processing concerning a specific person is changed after an objection is made does not automatically mean that the data processor has erred in the past. The data processor is simply ready to change the composition of the data they process if necessary and to comply with the requirements arising from legislation.

It must also be pointed out that the disclosure and/or transmission of data must be suspended until the objection is resolved (Article 21 (1) of the GDPR). The same is confirmed by Article 18 (1) of the GDPR – the processing must be suspended until it is clear whether the personal data is correct or until it is ascertained that the legitimate reasons of the controller override the reasons of the data subject. Suspension of the processing upon receipt of the objection means that the processing of the data (including transmission) is terminated until the valid legitimate reason for further processing has been assessed. If there is no such reason for further



processing under Article 21 (1), the processing must be stopped and, if there is, the result of the analysis and the decision on further processing must also be communicated to the data subject (Article 18 (3) and Article 21 (1) of the GDPR).

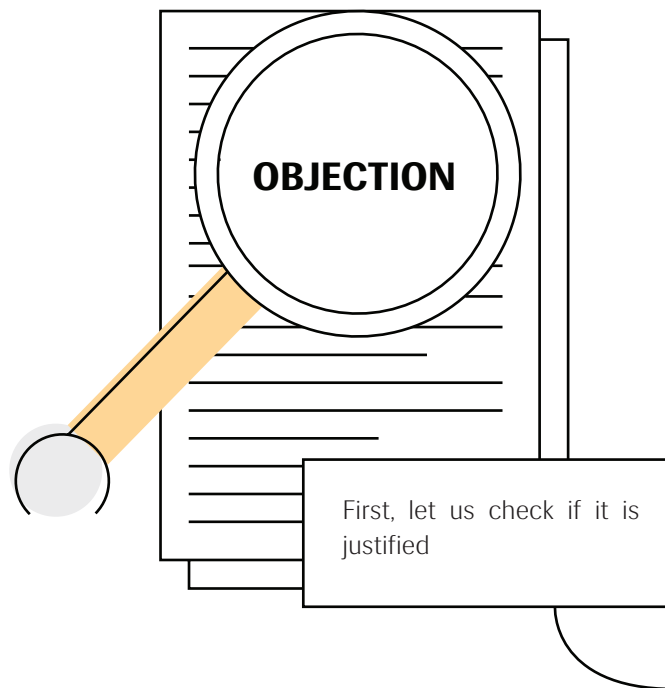
Each data subject also has the right to object to the fact that the third party did not have a legal basis for obtaining the data. In this case, it must be determined whether the objection is justified or not. If it transpires that the data was transferred unlawfully, the data processor is obliged to assess whether the unlawful transfer caused or is likely to cause a threat/damage or serious harm to human rights and freedoms. Depending on the outcome of the assessment, either the breach should be documented only, the Inspectorate should be notified in the event of a breach, or both the Inspectorate and the person whose data were processed unlawfully should be notified.

Each objection must be resolved on a case-by-case basis.

It must also be borne in mind that debt data cannot be disclosed on the basis of a legitimate interest if this would infringe the rights and freedoms of the data subject. However, publishers of debt data have often relied on a legitimate interest in justifying their activities.

A person has the following rights:

- right of access
- right to rectification
- right to erasure/to be forgotten
- right to restrict processing
- right to data portability
- right to object
- right to be informed
- rights in relation to automated decision making and profiling



It appears from the procedural practice of the Inspectorate that if the debt data of a data subject has expired, the data processor does not often terminate the publication of debt information. This is an example of infringement of the rights and freedoms of the debtor as a data subject. Often, the data subject is not informed at all about the transmission and publication of the data. Both the notification and the assessment of the justification of the data processing are the responsibility of the controller. If they fail to fulfil these obligations, a supervisory authority will interfere.

‘Every data processor, including both the registrar of the Credit Register and the portal operator, is obliged to follow the principles set out in Article 5 (1) of the GDPR and is responsible for their implementation. If there is no legal basis for the processing, the processing of personal data must be waived.’

A COMPANY HAD TO REMOVE DEBT DATA FROM THEIR WEBSITE

Last year, there were several cases when a company disclosed the names of people and the amounts they owed on its website. In the yearbook, the Inspectorate describes the process of reaching a procedural decision on the example of a case regarding a tour operator. However, the principle in the processing of debt data is always the same. Namely, the tour operator published the debts of its customers on its website.

When processing personal data, the requirements of the Personal Data Protection Act and the General Personal Data Regulation must be taken into account. Among other things, the data processor is obliged to follow the principles set out in Article 5 of the GDPR, including the provisions of subsection 1 (a), (b), and (c):

- personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- purpose limitation – personal data is collected for specified, explicit, and legitimate purposes;
- data minimisation – personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

The fulfilment of obligations must be proved by the controller on the basis of Article 5 (2) of the GDPR.

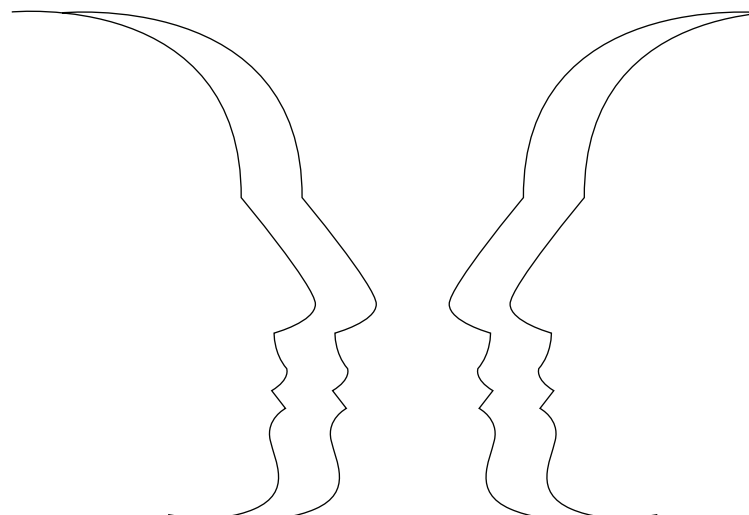
Personal data may be processed only to the extent necessary to achieve the defined purposes, whilst ensuring that the purpose of the processing infringes fundamental human rights as little as possible.

The data processor must always assess in advance whether the processing of data (including disclosure) is indispensable for the fulfilment of the purpose or whether it is possible to use less intrusive measures to fulfil the purpose.

In addition, section 10 of the Personal Data Protection Act must also be taken into account when processing personal data in connection with a breach of an obligation. Pursuant to subsection 10 (1) of the Personal Data Protection Act, *'transmission of personal data related to violation of any obligation to third parties and processing of the transmitted data by any third party is permitted for the purpose of assessment of the creditworthiness of the data subject or for any other similar purposes and only in the case the controller or processor has verified the accuracy of the data transmitted and the legal basis for transmission of personal data and registered the data transmission.'*

Based on the above, it is prohibited to disclose the data of debtors on the website and the transfer of data is permitted only if the conditions provided for in subsection 10 (1) of the Personal Data Protection Act are met. In addition, subsection 10 (2) of the Personal Data Protection Act, which stipulates conditions prohibiting the transfer of data, must also be taken into account before transferring data.

As the tour operator did not take into account the above requirements when processing the debt data, it violated the requirements of the Personal Data Protection Act and the GDPR when disclosing the debt data. The procedural decision of the Inspectorate required the removal of personal data related to the breach of the obligation from the website.



RETENTION OF PERSONAL DATA FOR 10 YEARS FOR THE PURPOSE OF DETECTING NEW FRAUD

The Inspectorate had an international case in which a company providing ride-sharing services distributed referral codes to ride service providers (customers of the company) on the basis of which it is possible to invite a new person as a customer of the company and receive a one-time bonus. However, one of the customers used a referral code between their two devices, i.e. they invited themselves to (re)join the platform of the company. The company blocked their account and the customer could not use the services of the company with their account. Based on the case, the company considered it necessary to keep the personal data for the purpose of detecting new fraud for 10 years, and the request of the person to have their data deleted after the end of the customer relationship was not satisfied.

The reason why the Inspectorate talks about this case in the yearbook is that a person has the right to demand that the controller delete personal data concerning them without undue delay if there are no longer grounds for processing personal data (see Article 17 (1) of the GDPR). For example, if the data have been collected in the course of the provision of a service but the provision of a service to a specific person has ceased, there is no legal basis for processing personal data and they must be deleted unless one of the circumstances set out in Article 17 (3) of the GDPR occurs.

In accordance with Article 17 (3) of the GDPR, paragraphs 1 and 2 do not apply to the extent that the processing of personal data is necessary:

- a) for exercising the right of freedom of expression and information;
- b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject;

However, the processing of personal data (including storage of data) on the basis of the mentioned point (b) is permitted if the obligation to process personal data arises from a specific law (e.g. subsection 12 (1) of the Accounting Act). In this case, the data may be processed only for the purpose provided for in the specific law (e.g. only for the purpose of storage). However, with regard to section 146 of the General Part of the Civil Code Act, the limitation period for a claim arises from this section and no direct obligation (statutory obligation) to store data arises from it. In addition, the company did not refer to any other specific law that would impose a legal obligation to process data for 10 years, including the right/obligation to store data for 10 years for the purpose of detecting or preventing fraud. The Inspectorate is also not aware of such a specific law.

- c) for reasons of public interest in the area of public health;
- d) for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes;
- e) for the establishment, exercise, or defence of legal claims.

Point (e) only applies if the processing of personal data is necessary for the establishment, submission, or defence of legal claims. In order for the person and the supervisory authority to be able to assess the above, the company must prove that the data processing is necessary for the specific person and that the data processing also complies with the requirements set out in Articles 5 and 6 of the GDPR.

In this case, Article 17 (3) (a), (c), and (d) of the GDPR were not suitable as a basis for data processing. The processing of data under point (e) requires an analysis of legitimate interests. Although the company sent an analysis of legitimate interests to the Inspectorate, it was based on the detection and prevention of fraud. However, for this purpose, it is not justified to store personal data for 10 years. Thus, the Inspectorate did not have an analysis of the company that would justify the storing of data for 10 years. The Inspectorate also had doubts that a 10-year storing of data could be necessary and justified in view of a specific breach.

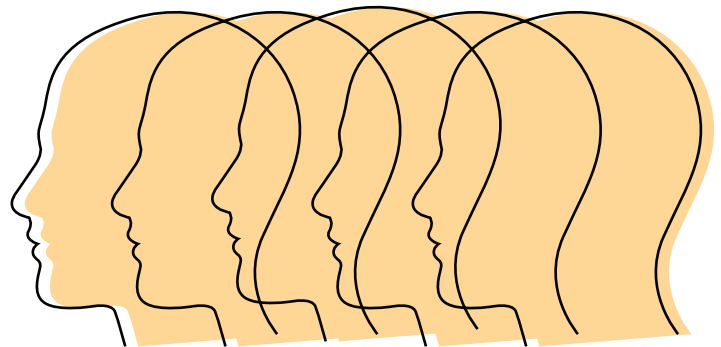
The Inspectorate found that to detect and prevent fraud and/or avoid further fraud, the company does not have the right/obligation to process the data for 10 years (including store, use).'

In the course of the proceedings, the company deleted the personal data of the complainant, with the exception of the documents which have to be stored in accordance with the Accounting Act.

In the context of this case, it is important to emphasise that the data processor is generally obliged to delete personal data when the data is no longer needed for the purpose for which it was collected. However, if the request to delete the data of the data subject is not granted, the data processor has the obligation to prove to the person and, if necessary, to the supervisory authority, for which legitimate reason the data processing is continued for the purposes of Article 17 (3) of the GDPR. In that regard, it is not sufficient to merely refer to a provision of the law, but the data processor is obligated to prove that that provision is applicable to the specific case and the specific data subject.

DATA PROTECTION IN EMPLOYMENT RELATIONSHIPS

In recent years, one of the most discussed issues has been data protection in employment relations, and the year 2020 was not any different. The Inspectorate was contacted primarily in connection with the organisation of video surveillance, but also in connection with issues related to access to employee data and closures of email addresses. Although the Inspectorate has addressed these issues in previous yearbooks, the basics should still be repeated.



LEGAL BASIS FOR MONITORING EMPLOYEES

The Inspectorate has often had to remind employers that personal data is any information that can be used to directly or indirectly identify a person. In practice, there have been situations where the employer wishes to monitor the activities and movements of the employee, but the fulfilment of work obligations can only be monitored in a way that does not violate the fundamental rights of the employee. Such processing of personal data can take place on the basis of a legitimate interest of the employer.

As a rule, personal data is processed during the employment relationship for the performance of the contract with the employee.

However, monitoring their emails, Internet usage, etc., is subject to the legitimate interest of the employer. Although the monitoring of an employee is closely linked to the obligations arising from the employment contract, it is at the same time certainly not necessary for the performance of the employment contract. The consent of the employee can be the basis for the processing of personal data in employment relationships only in cases where the processing of personal data is not unavoidable and the employee can actually decide whether they want to consent to the processing of personal data and have the possibility to withdraw it.

Relying on legitimate interest presupposes that the employer has carried out and documented in writing a

thorough assessment and consideration of the interests. This includes assessing whether it is sensible and necessary to read emails and monitor the use of the Internet and other programs. In this situation, we recommend setting the rules for using email, the Internet, and other programs.

This also applies, for example, to software installed on a computer of an employee which, after a certain period of time, takes screenshots of the image on the computer screen of the employee and sends them to

the employer who then stores those image files (in association with the persons concerned). This also applies in a situation where the employer requires the employee to install an application on their personal phone that monitors their movement or in a situation where the employer installs a GPS device in the work vehicle and the user of the vehicle is identifiable.

DATA PROCESSING BEFORE AND AFTER AN EMPLOYMENT RELATIONSHIP CAUSED CONCERNS

The Inspectorate received several inquiries concerning the processing of personal data when applying for a job. The general basis for processing the personal data of a candidate is their consent. However, data about the candidate may also be collected without their consent (for example, from public sources that the candidate has published on social media, etc.). In addition, the potential employer has the opportunity to contact the previous employer, but only if the person has given their explicit consent.

Access to email

However, the Inspectorate was contacted more in regards to the processing of data after the end of the employment relationship. Most questions were about the personal email addresses of former employees. As a rule, the employee is given a personal email address to perform the tasks specified in the employment contract. After the termination of the employment relationship, the original legal basis for processing the email address of the employee (no employment contract) is no longer valid. After the termination of the employment relationship, the processing may be based on the consent of the employee (if no rules for the use of email had been established in the company) or, if there are rules on the use of email, the legitimate interest of the employer.

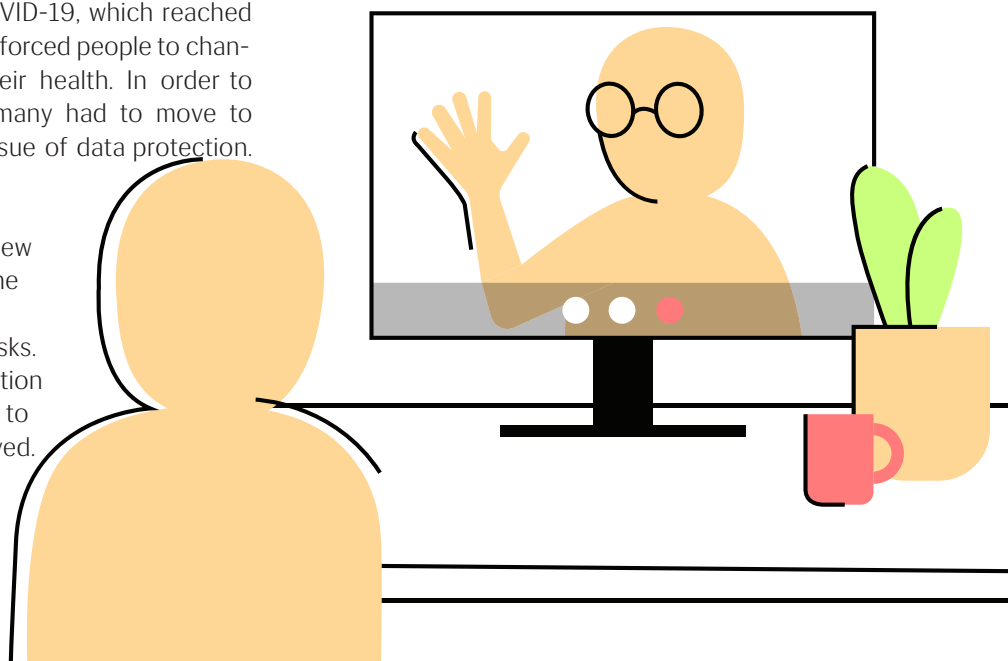
The employer can easily store and read emails related to the performance of work duties that were sent to and from the business email address of the employee during the employment relationship (contract). However, the employee does not have the right to open or read private emails. In order to prevent or reduce the likelihood that private messages will be read, rules for using the email account must be established. For example, the use of the business email address for personal purposes may be prohibited and rules may be laid down for the storage and deletion of private emails in a separate folder.

It should be noted that the more detailed and specific the rules are, the easier it is for the employee to follow them. It must be borne in mind, however, that the rules cannot impose restrictions or create rights for the employer that are contrary to the constitution or other laws.

If the rules for using email are not regulated in the company and the former employee does not give consent to keep the email open, their personal email address should be closed immediately after the termination of employment. Closing an email address means that emails cannot be delivered to that address. If the employer has not closed the personal email address of the employee and there is no legal basis to keep it open, the person has the right to request the deletion of their personal data from the employer pursuant to Article 17 of the GDPR.

DATA PROTECTION DURING THE CORONAVIRUS PANDEMIC

The coronavirus disease, or COVID-19, which reached and spread in Estonia last year, forced people to change their way of life to protect their health. In order to continue working and studying, many had to move to virtual spaces, which raised the issue of data protection. The coronavirus was like a cold shower in the morning for the society, but it had to adapt to the new situation quickly. This meant that the Inspectorate also had to gather its strength and face the additional tasks. The yearbook only includes a selection of topics that the Inspectorate had to address when the coronavirus arrived.



EMPLOYERS, EMPLOYEES, AND HEALTH DATA

The coronavirus brought numerous requests for explanation to the Inspectorate regarding the processing of the health data of employees. Health care institutions, schools, production and entertainment companies, and many others submitted their questions. The Inspectorate was able to provide explanations in accordance with the applicable national law. The GDPR allows the processing of health data in the context of an employment relationship to the extent permitted by the law of a Member State which also lays down appropriate safeguards.

Information on the state of health of an employee is a special category of personal data to which Article 9 of the GDPR applies. This is also the case if there is a suspicion and not a definite diagnosis. Talking about having a cold also means the processing of health data within the meaning of the law.

Health data may be processed only on the basis set out in Article 9 (2) of the GDPR.'

Article 9 (2) (a) of the GDPR refers to consent under which an employer may process both regular and special categories of personal data. The basic

requirement is that the consent requirements of the GDPR are met, including that the consent has indeed been given voluntarily. The employee must not be subject to any pressure to give their consent or be penalised for not giving it.

Article 9 (2) (c) of the GDPR refers to the processing of special categories of personal data where this is necessary to protect the vital interests of others and the data subject is not physically able to give consent (e.g. due to their medical condition). Theoretically, this seems to provide a basis for informing employees even without consent, but the principles of purpose limitation and minimisation must still be followed. In other words, personal data may not be transferred if the purpose can be achieved otherwise.

Requirements for employers and employees

The employer must ensure a safe working environment. The requirements for this arise from the Occupational Health and Safety Act. However, this legislation does not regulate exactly whether and what health data can be collected about an employee. The general view is that employee data should be requested and collected as much as necessary and as little as possible.

An employee must keep in mind that they can only start working if they are healthy and do not pose a risk to other employees. The employer has the right to ask whether the employee has recently been in a risk area or has come into contact with infected people.'

This includes the right of the employer to request confirmation, which does not mean that the employer should be given the detailed diagnosis of the employee. Information on the occurrence of symptoms should also be exchanged by mutual understanding.

Employers often wanted to inform collectives about infections and asked if the employer could send a substantive notice to all employees, using the name of the employee if they had given their consent. The processing of health data must respect the principles of purpose limitation, minimisation, proportionality, and fairness, so it is not clear why it is necessary to send a personalised message to all employees who may not have been in contact with the infected employee.

The identification of those who have been in contact with the infected person should take place in such a way that the employer does not inform the whole team about the person, but tries to find out and inform the persons who have been in contact with the infected employee. The same must be done with people outside work – e.g. if a joint meeting has taken place.

Pursuant to subsection 14 (1) of the Occupational Health and Safety Act, an employee is required to:

1. contribute to the creation of a safe working environment by observing occupational health and safety requirements;
2. make correct use of the prescribed personal protective equipment and keep it in working order;
3. promptly notify the employer or the representative of the employer and a working environment representative of an accident or a risk thereof, of an occupational accident, or their health disorders which impede the performance of their duties, and of any shortcomings in the protection arrangements.

To do this, the employer should first ask the affected employee themselves about the people they have had sufficient contact during the potentially infectious period for the spread of the disease, and then talk to these employees in person. If it is not possible to contact the sick employee, the employer should analyse who could have been in close contact with them (common room, meetings).

The employer sending a warning email to all employees with the content 'Mart has stayed on sick leave and it is possible that he has COVID-19' is not justified.

Informing other employees of the illness is permitted only if the communication of such information to other employees is necessary for the protection of their life, health, or liberty and the consent of the sick employee cannot be obtained.'

Why can an employer not ask for the diagnosis of an employee?

It is the task of doctors and the Health Board to diagnose the virus and ascertain the mode of the infection and identify the persons who have been in contact with the infected person. Therefore, the doctor who diagnoses a patient with the coronavirus should also ask the person with whom they have been in contact. The matter can be further dealt with by the Health Board, which also has the right to process personal data for this purpose, including receiving it from the employer.

Therefore, the Inspectorate pointed out that no other data processor has a legal basis or purpose arising from law to start collecting or transmitting additional data on its own initiative to someone who does not have the right to process it.

Pursuant to the law, the health care provider (see clause 6 (1) 3) of the Communicable Diseases Prevention and Control Act [2]) and the Health Board (clause 18 (1) 1) of the Communicable Diseases Prevention and Control Act) have the right and obligation to ascertain the mode of the infection and identify the persons who have been in contact with the infected person. The latter also has the right to process personal data for this purpose, including receiving it from the employer.

DATA PROCESSING DURING THE CORONAVIRUS PANDEMIC IN ENTERTAINMENT ESTABLISHMENTS

The Inspectorate received several questions as to whether entertainment establishments have the right to provide the Health Board with the data of the person who participated in the event (email address, telephone, name) if there is reason to suspect that a person infected with the virus participated in the event.

Pursuant to subsection 18 (1) of the Prevention and Control of Communicable Diseases Act, the Health Board has the task of ascertaining the circumstances under which persons suffering from a disease became infected, determining the circumstances of the spread of the communicable disease, and, if necessary, contacting persons suffering from a communicable disease and the persons who have been in contact with the infected person.

For this task, the Health Board has the right to ask the organiser of the event (entertainment establishments) for the data of the participants in the event, provided that the organiser has their personal data (e.g. the customer used a customer card when purchasing a ticket). The Health Board can request this information purposefully, i.e. to identify the persons who were in contact with the infected person at the event. It is presumably not necessary to have the data of all the people who participated in the event.

However, entertainment establishments do not have the right or reason to transmit the data of all the participants in the event on their own initiative. Entertainment establishments do not have the capacity to assess the state of health in such a way that there are sufficient grounds to suspect a visitor specifically of the coronavirus and to inform the Health Board thereof.

VIEWING THE HEALTH DATA OF PEOPLE INFECTED WITH CORONAVIRUS MEANT A WARNING

The Inspectorate received several complaints against the medical chief of Kuressaare Hospital, who had made inquiries about the health data of people in the Health Information System. By the order of the Board of Kuressaare Hospital, the medical chief was required to perform an audit of the COVID-19 samples taken in the information system of the hospital. According to the hospital, Kuressaare Hospital is a vital service provider that must ensure the provision of both ambulance and hospital services on Saaremaa even in an emergency situation, and therefore the hospital needed to know how many people had given a positive coronavirus test on Saaremaa to ensure their ability to provide medical care.

The Health Services Organisation Act and its regulations set out very clearly who has the right to view data from the Health Information System and in which cases. In the course of the supervision procedure, the Inspectorate established that the directive of the Board of Kuressaare Hospital obliged the medical chief to conduct an emergency audit because the test results of the COVID-19 samples had not arrived at the hospital on time and an overview of COVID-19 patients in the Saaremaa rural municipality was needed. Considering the emergency situation caused by the coronavirus pandemic and the resulting confusion, as well as the fact that the inquiries were not made out of curiosity, the Inspectorate did not punish the medical chief for misdemeanour. The Inspectorate warned the medical chief for exceeding his powers.

THE POSSIBILITY OF COOPERATION BETWEEN TWO AUTHORITIES DURING THE CORONAVIRUS PANDEMIC REQUIRED AN ANALYSIS

Last year, the Inspectorate analysed the competencies of agencies in processing personal data in the performance of its task on several occasions. Last year, the Inspectorate also helped to answer the question of how and on what basis the Health Board transmits data of people infected with the coronavirus to the Police and Border Guard Board.

The result is worth addressing because data protection enthusiasts also read the yearbook.

Pursuant to clause 18 (1) 1) of the Communicable Diseases Prevention and Control Act, the competent authority in the area of the prevention, surveillance, and control of communicable diseases is the Health Board which, among other things, conducts epidemiological investigations with the aim of ascertaining the circumstances under which persons suffering from a disease became infected and of determining the circumstances of the spread of the communicable disease, contacts, if necessary, the persons suffering from a communicable disease and the persons who have been in contact with the infected person, and, in the event of clusters of disease, provides instructions for the application of disease control measures. Subsection 18 (6) of the Communicable Diseases Prevention and Control Act stipulates that in performing the functions prescribed by the Act, the Health Board cooperates with local governments for the prevention and surveillance of communicable diseases and to prevent and control the spread of communicable diseases.

Pursuant to clause 3 (1) 1) of the Police and Border Guard Act, the functions of the Police and Border Guard Board are the prevention of offences provided for in Chapters 9, 12, 13, 16, 17, 21, and 22 of the Penal Code, unless this function has been assigned by another Act to another administrative authority and on the basis and pursuant to the procedure provided for in the Law Enforcement Act. This also includes section 192 of the Penal Code, which provides the norm for causing the threat of the spread of an infectious disease or infectious animal disease. In order to prevent this offence, the Police and Border Guard Board needs data from the Health Board. The function comes from subsection 24 (2) of the Emergency Act.

Pursuant to section 7⁴⁶ of the Police and Border Guard Act, in order to perform the tasks provided for in subsection 3 (1) of the same Act, as well as for the performance of tasks arising from an international agreement or European Union legislation, the police have the right to process personal data, including special categories of personal data and data available to the public and available from public sources. This norm is an authorisation to process personal data, which presupposes that a task arises from law for the performance of which the processing of personal data is necessary. With regard to the transfer of data to the Police and Border Guard Board, clause 18 (1) 2) of the Administrative Co-operation Act must also be taken into account, in accordance with which an administrative authority may request professional assistance from another administrative authority if information which the administrative authority does not have or is unable to ascertain is required for the performance of a particular administrative duty.

The Health Board provides the Police and Border Guard Board with the data of the persons suffering from a communicable disease and the persons who have been in contact with the infected person because the Police and Border Guard Board does not have them and without them, it is not possible to perform the task arising from law.'

SCREENSHOTS OF A VIDEO CONFERENCE ON SOCIAL MEDIA CAUSED ISSUES

Due to the coronavirus pandemic, many employers had to rethink their work arrangements and allow employees to work from home. In a situation where many worked from home and often communicated through video calls, people started sharing their thoughts and observations about the situation on

social media, often with pictures. But first, it is necessary to ask the colleagues for permission or change the picture before posting so that they are no longer recognisable. Thus, the Inspectorate also had to deal with simpler reminders to emphasise the importance of information security so that the data of no one would leak against their will.

MEDIA AND COVERING CORONAVIRUS TESTING

Understandably, the issues related to the coronavirus crisis also received a lot of media attention in 2020. Especially during the first wave of spring, there were a lot of photos and video material from coronavirus testing points. Often, however, the people seen on the material were recognisable. As a rule, cars were photographed, but the people sitting in the car were also visible on the images and in videos. These people were often disturbed and asked for help from the Inspectorate. A news story was also published with a large gallery of unmasked people who visited the shopping centre. The people were identifiable from the pictures.

The Inspectorate had a case where a journalist wrote an article about the everyday life of a special care home and added a photo gallery of people with special needs who live there. The relatives of the residents found out about the visit and the photos only after reading the article and turned to the Inspectorate to complain.

The Inspectorate proposed to the publication to blur the faces of the people and other data that could be used to identify them from the images or video. Personal data may be processed for journalistic purposes without the consent of the person, provided that this is in the public interest and in accordance with the principles of journalistic ethics and that the disclosure of personal data does not unduly prejudice human rights. The Supreme Court has clarified that the use of an image of a person without their consent is generally permitted only to reflect a current event related to that person. However, the presumption that the use of an image of the person is necessary to reflect the event and that the public interest outweighs the interest of the person must also be taken into account here¹.

According to the Inspectorate, it does not follow from the court judgment that images of people can no longer be used with news.'

A recording of random people in a public place used with the article or news must not in any way give the impression that the news is about the specific people seen on the recording.'

Sensitive places (such as the Unemployment Insurance Fund, hospital, special school) should be photographed for news stories in a way that does not compromise the privacy of people. If there is no public interest in a particular person when photographing in such a place, the person should either be photographed in a way that ensures they are not recognisable or the person should be given the opportunity to avoid being captured.

In conclusion, it is not permitted to disclose personal data for journalistic purposes without the consent of the person without there being a public interest in the disclosure of the data of that particular person. Obviously, there was a public interest in covering the coronavirus testing and similar topics, but this did not justify the fact that people who happened to be in front of the camera were recognisable.

¹ Judgment of the Supreme Court in case No. 3-2-1-152-09.

DISTANCE LEARNING WAS DIFFICULT IN TERMS OF DATA PROTECTION

The coronavirus brought a new situation to the field of education, and despite their digital competence and technical readiness, everyone had to transition to distance learning in a short time, which also caused a lot of data protection issues. The Inspectorate gave guidelines to all schools, and a video seminar for educational institutions was held in autumn. When transitioning to distance learning, it was first necessary to find out the legal basis for the data processing in a video lesson. In addition, dozens of other issues related to access and recording had to be addressed.

The streaming of classes in the case of blended and distance learning takes place for the performance of a public task and does not require prior consent.

In the case of distance learning, all studies take place virtually for the purpose of organising studies. However, in the case of blended learning, there should always be a real need (e.g. an agreement with a parent whose child must be quarantined, sick leaves, etc.). It is up to the school to decide whether and under what conditions anyone will be offered a blended learning opportunity.

It is always possible to use separate communication with the teacher for absent children, such as with home schooling, or to temporarily provide the opportunity to retake assignments and offer counselling. It is technically difficult to conduct blended learning because the teacher moves around the classroom and is not constantly in front of the camera, their voice is not always heard, and the background noise makes it difficult to listen to the teacher. This way of teaching may not provide the desired goal. However, communicating with the class via video helps the student to feel that they are part of the class. The Inspectorate pointed out that the installation of any stationary camera in the classroom is not justified in the case of blended learning.

Only designated persons can have access to the broadcast. If the service makes it possible, access to the environment could be further protected with a password. The teacher should be able to make sure that the video is only viewed by the intended children, meaning that even the parents cannot watch is without prior agreement. The teacher may require the student to turn on their camera as well. If the goal is to attend a class and conduct a class, there is no reason to record it. If a student is absent from class, they should retake it like they would in contact learning.

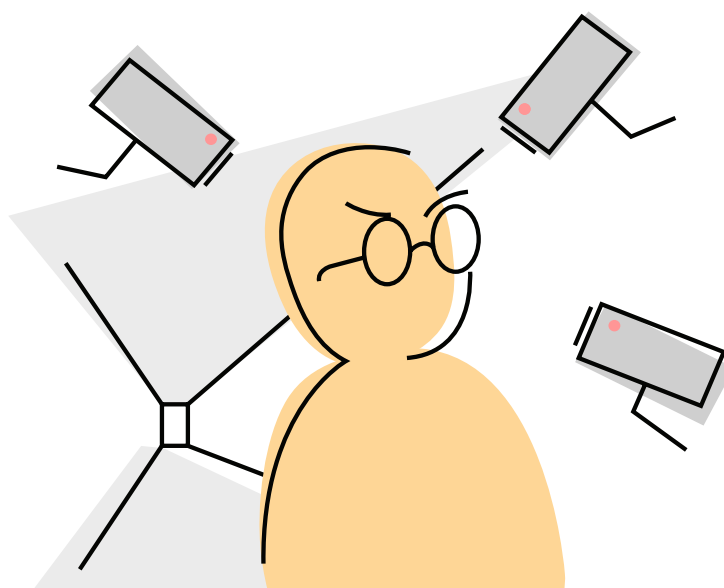
WHY HAS THE USE OF SECURITY CAMERAS BECOME A PROBLEM?

Last year, the Inspectorate also received a large number of appeals from people regarding video surveillance by their neighbours. Conflict is usually caused by either not knowing of who is watching you or a perceived invasion of privacy.

‘The house is co-owned and one day, a neighbour installed a security camera without asking me.’

‘The cameras are filming the sports field, but I do not know whose camera it is.’

‘The neighbouring lot has garages and one of the garages has a camera on top of it that is directed into my window. I live on the first floor and feel that my right to the integrity and privacy of my home has been violated.’



'The building has security cameras that also film the gardens in the neighbouring lot. The residents are not okay with this and we demand that the cameras be removed immediately.'

In 2020, the Inspectorate started more systematic information work so that video surveillance organisers could take better account of human rights and so that their activities would be transparent.

In cooperation with the Centre of Registers and Information Systems, an IT-based video surveillance sign generator was completed. To do this, it was necessary to map out the minimum information requirements that each sign should contain. The requirements for the sign arise from Article 14 of the GDPR.

VIDEO SURVEILLANCE IN COMMON AREAS

As security cameras often cause problems in Apartment associations, the Inspectorate compiled a comprehensive article on how to operate security cameras in residential areas and published it on the website aki.ee ('Kaamerate kasutamine elamualadel – www.aki.ee).

One of the aims of the article was to make people think about whether the use of a security camera fulfils its purpose and how to use the camera in a way that does not unduly infringe on anyone's right to privacy.

Some important facts in the article

When using a stationary camera, personal use is only allowed if you only film the area you own (your own apartment or only the door of your own apartment or your own private house and its yard). In this case, it is not necessary to inform anyone, but the recordings may not be used for any other purpose than personal use (e.g. publishing on the Internet). Thus, when using a stationary camera for a personal purpose, it cannot be used to film a public or shared area, such as a street, an apartment building staircase, an adjoining yard, etc.

The decision should always include an assessment of the severity of the hazards and the likelihood of their occurrence, as well as an analysis of alternatives to mitigate security risks (e.g. security door, alarm, additional lighting). For example, if you want to protect bicycles stored in the stairwell from being stolen, you have to install the camera so that only the storage area of the bicycles is visible, which means that you do not have to install cameras on all floors of the stairwell. If, after the assessment, it appears that other security measures have been exhausted and that the installation of cameras is

The purpose of the video surveillance, the legal basis, the name of the controller, and information on where the person entering the surveillance area can read the conditions of data protection or ask about the processing of their personal data must be indicated on the sign.'

unavoidable, their presence must not unduly infringe on the privacy of any apartment owner (e.g. the camera films one particular door). Pay attention to which area has to be in the field of view of the camera and whether the camera has a zoom and audio recording function in addition to the image, etc. There is no reason to use a camera that records audio in protecting your property. Potential thieves are unlikely to talk near the camera, so this feature does not make it easier to find them but unduly compromises the privacy of other people on the recording.

Judgment of the Court of Justice in Case C-708/18 states that when assessing the necessity of processing, the controller must, for example, assess whether it is sufficient for the video surveillance system to work only at night or outside normal business hours and to block or blur video images in places where video surveillance is not required.'

The decision of the association must be adopted at a general meeting with the right to vote and the decision of the board along is not enough.

The Inspectorate pointed out that the use of a dummy camera or an unconnected camera gives people the impression that they are being filmed, which is why the owner of such a device must be prepared to give explanations to both the people in front of the camera and the supervisory authority.

VIDEO SURVEILLANCE IN TOILETS

The Inspectorate also received complaints about cameras installed in toilets. For example, the Inspectorate issued a precept-warning to the Rakvere Kroonikeskus Centre to remove the cameras installed in the toilets. As a result of an inquiry of the Inspectorate, cameras were also removed from the toilets of the Park Centre in Jõhvi.

The Inspectorate continues to take the view that it is not acceptable to use cameras in lounges, changing

rooms, toilets, and showers, including in offices and shopping or sports centres. In situations where the aim is, for example, to prevent vandalism or incidents involving the handling or use of a narcotic substance, it is essential to consider alternative measures that are less intrusive on the privacy of individuals than the use of surveillance devices.

CONFUSION AMONG EMPLOYEES

One of the biggest problems was the fact that the data processing is not transparent. The employees have not been properly informed and there is often no information in the rules of work organisation. Personal data may be processed with the use of cameras on legal grounds – for example, on the basis of legitimate interest or if the obligation to use the cameras arises from a specific law. Legitimate interest as a basis for the processing of personal data can only be invoked if the data processor has weighed up the interests of the employee and the employer and concluded that the use of cameras does not unduly prejudice the interests of the employees.

Legitimate interest as a basis for the processing of personal data can only be invoked if the data processor has weighed up the interests of the employee and the employer and concluded that the use of cameras does not unduly prejudice the interests of the employees.'

One of the most important requirements is to inform the people in the field of view of the cameras both about the legal basis of data processing and the more precise purposes of surveillance, including allowing the employees to inspect all relevant documents. Unfortunately, the past year showed that this is often not the case. However, the employer must be able to provide information and explanations to employees at all times. There must also be signs informing the people that the area is being filmed. As we receive many questions and complaints on these topics, a number of explanatory materials for the video surveillance organiser have been added to the website of the Inspectorate.

In summary, the employer must:

- (a) document the assessment of legitimate interest,
- (b) indicate the data protection conditions setting out the conditions and purposes of the use of the cameras; and
- (c) install video surveillance signs.

ELECTRONIC DIRECT MARKETING AND TELEPHONE SALES CONTINUED TO CAUSE MANY COMPLAINTS

Spamming continued to be a problem last year. The complaints reflected that the problem was still obtaining the email addresses of various natural persons and sending emails to them without their prior consent. Often, the data processors did not give explanations as to from where the email address was obtained and on what legal basis the email was sent to the person.

Last year, problems were also caused by forest businessmen who called people in the hope of buying a property or helping to sell an existing plot of land.

The data on land is obtained from the land register and all kinds of other databases. However, it is questionable from where the mobile phone numbers of natural persons are obtained. In some cases, they are obtained from the commercial register if someone has added their personal number to their business, members of their apartment association,

and so on.

However, there are also situations where the phone number of the person is not publicly available anywhere, but the caller even knows their name and that they own the registered immovable. For example, there was a call to a child of a landowner. The caller knew that the parents of the person picking up the phone owned a registered immovable. Interestingly, data processors have stated that the numbers are randomly generated. Another standard answer is that the number is derived from an old database that no longer exists.

Collecting telephone numbers from random databases is not in line with the initial purpose of their disclosure. Therefore, it is not allowed to collect numbers from databases in order to start calling them. If a number is published for the purpose of selling a used car, it is not permitted to call the person and offer them the opportunity to sell their registered immovable or try to sell them vacuum cleaners, for example.

Telephone salespeople, who call computer-generated numbers without knowing who will answer the call, also continued to cause problems. The Inspectorate also received such complaints, but we cannot help these people as not all sales calls can be avoided. It is, however, possible to ask the company not to call you again.

In addition, when legal persons contact the Inspectorate with the concern that they are sent electronic direct marketing without their prior consent, all we can do is explain the situation. While a natural person must first give consent to be sent advertisements, it is possible to send them to a legal person without prior consent. However, the email must include an unsubscribe link. If a new email is sent after unsubscribing, it is a violation of the requirements of the Electronic Communications Act.

If Estonia imposed administrative fines, the proceedings would certainly be more efficient. We talked about the problem with serial spammers in more detail in the yearbook of 2019.



MORE CLARITY WAS EXPECTED FROM THE CONDUCT OF STUDIES FOR POLICY DEVELOPMENT

The Inspectorate issues permits for conducting studies for policy development. Last year, we issued 32 permits. During the processing of permit applications, it became clear that the organisers of the studies do not want to inform the data subjects about the studies. There are many reasons for this, from unreasonably high workloads to high costs.

However, this may cause the individual as a data subject to feel that the process of conducting the study may be covert. The position of the Inspectorate is that it is not always necessary to inform the persons but the point of view of the persons should also be considered – we all want to know if something is done with our data, and we also have a legitimate expectation for that. The same issue has been pointed out by ethics committees.

The organisers of the studies should think about the sample size and assess the possibility of informing people. In e-Estonia, this is made easier thanks to the possibility of easily communicating with people electronically. Therefore, where possible, the organisers should make every effort to inform people about the processing of their data. Contact information is available either in the population register or often in databases. The Inspectorate is of the opinion that in the future, the organisers of studies for policy development should make a greater contribution to increasing the transparency of the processing of personal data.

PROCEDURE FOR DETERMINING THE RIGHT TO CARRY OUT BACKGROUND CHECKS: AIR CARRIER, AIRPORT, AND THE INTERNAL SECURITY SERVICE

Last year, the Inspectorate received an application for intervention in which the applicant requested clarification of the role of Tallinn Airport in reviewing the applications for identification cards of the air carrier Regional Jet OÜ to the Estonian Internal Security Service and whether there is a legal basis for this.

This is in violation of data protection principles. In practice, the employer only has to check for the presence of a container of encrypted files or a sealed envelope. The same principle applies to the applications for applying for personnel security clearance.

The opinion of the Inspectorate is shared by the Chancellor of Justice, who came to the opinion that the person to be inspected must be able to submit the questionnaire directly to the person performing the security inspection, either encrypted or in another way. Although the security check regulation does not currently provide for such a possibility, it is the one and only way in terms of data protection.

The reference to the obligation of the employer to verify compliance with the formal requirements of

the questionnaire must be interpreted in accordance with the principles set out in the GDPR and the Personal Data Protection Act. One such principle is data minimisation – as little data as possible should be collected to achieve the desired purpose. The Internal Security Service or the Foreign Intelligence Service decides on the granting of personnel security clearance, and in the opinion of the Inspectorate, a unit or person organising a state secret in an agency or enterprise may not examine special categories of personal data in the application. It must be acknowledged that clause 23 (5) of the 'Procedure for the protection of state secrets and classified information of foreign states' is poorly worded and the verification of compliance with formal requirements could seem to include the verification of the content of the questionnaire. However, if that provision is interpreted in the light of the GDPR and the Personal Data Protection Act, the check on compliance with the formal requirements must be limited to a check on the existence of files.

The questionnaire includes, among other things, very personal and sensitive information, such as alcohol and drug use (including trying them once), visits to a psychologist and psychiatrist, gambling, etc. The

personal data questionnaire thus clearly contains special categories of data, the processing of which is more strictly regulated. Among other things, data on former and current partners can be qualified as special categories of data, from which conclusions can be drawn about sexual orientation. As a result, very personal and deeply intrusive personal data, in the sense of the GDPR, are processed. Therefore, special attention must be paid to the principles of personal data processing arising from the GDPR and the Personal Data Protection Act. In order to identify deficiencies, it is not necessary for the structural unit of the employer to examine the data in the questionnaire; these deficiencies can be pointed out by the agency which performs security checks itself.

If there are any deficiencies in the questionnaire, thanks to procedural economy and the principle of data minimisation, the agency which performs security checks can communicate directly with the

person. This solution is faster and less burdensome for the parties. Furthermore, the administrative relationship arises between the applicant and the agency which performs security checks, not between the agency which performs security checks and the employer, as the identification card is issued to a person and not to the authority or company.

The Inspectorate issued a precept to the airport in which it obliged the airport to submit the personal data questionnaire of the applicant for the identification card of the employees of the air carrier to the Internal Security Service in encrypted or sealed envelope in accordance with section 469 of the Aviation Act. The Airport is also not allowed to make a copy of the paper questionnaire, and paper copies of the collected personal data questionnaires must be handed over to the Internal Security Service or destroyed if the Internal Security Service does not need them. The airport complied with the precept of the Inspectorate.

WHY HAS MY HEALTH DATA BEEN VIEWED?

The year of the coronavirus pandemic increased the awareness of people in regards to their health data and therefore, they were more skilled in monitoring their patient portal logs more, which made them wonder if their health data had been viewed for good reason.

Last year, we had many complaints about the viewing of health data in the patient portal due to a software bug in a new service. The Health and Welfare Information Systems Centre (TEHIK), in cooperation with the Ministry of Social Affairs and the Family Physicians Association of Estonia, created a service where family physicians can make a practice list-based query to the Health Information System for all the patients in the practice list regarding COVID-19 test results. However, the program made queries to the Health Information System at close regular intervals, resulting in an unreasonable number of logs.

The Inspectorate had an informative role to play in this solution, as many people were not sure who to turn to with their questions. We passed on the information received from the Health and Welfare Information Systems Centre as clearly as possible and kept up to date with the situation to ensure a comprehensible overview of who makes inquiries into the health data of persons and for what reason.

In most cases, the Inspectorate was able to confirm that the purpose of an 'unnecessary' inquiry was not to obtain information on a specific patient, but the system simply displayed the names of all those who took the COVID-19 test. It is then possible to find out from the logs whose health data has actually been viewed by health care providers.

The Inspectorate also initiated misdemeanour proceedings on the basis of subsection 71 of the Personal Data Protection Act due to illegal processing of health data.

As in previous years, the reason for initiating the procedure was the interest of medical staff, above all, in the health data of their relatives or acquaintances, which often made the procedure emotional and more complicated than usual. The Inspectorate had to ensure that both parties were equal and do everything possible to ensure that health care providers who violated the rule of law understood the illegality of their actions.

Health care providers and persons involved in the provision of health services must not take advantage of their position. Access to special categories of personal data is meant only for the provision of health services and, unlike health care professionals, other people do not have access to health data. Therefore, there is no justification for taking advantage for personal gain as allowed by the legislator in this manner.

The procedural fines were not high, but account has been taken of the fact that people generally understood what they had done wrong and the fine has been used as a tool to prevent similar situations in the future. In some cases, summoning a person to testify was already a sufficient punishment.

THE RIGHT OF SUCCESSORS TO RECEIVE HEALTH DATA

The Inspectorate received further questions related to health in addition to the worries of people in regards to their health data being viewed. One of the most important examples is successors requesting health data of their deceased loved ones. Often, hospitals did not provide people with the health history of their deceased loved ones.

In accordance with section 9 of the Personal Data Protection Act, the personal data of a deceased person can be processed with the consent of their successor. The question arose as to the proof that a succession certificate provides. People were concerned that the succession procedure could last up to 30 years, but this is a limitation period for claims arising from the General Part of the Civil Code Act, and the succession procedure itself will certainly not last that long.

In order to understand this, it is necessary to look at the Law of Succession Act which states that with the acceptance of a succession, all rights and obligations of the bequeather transfer to the successor except those which by their nature are inseparably bound to the person of the bequeather.

In its decision 3-20-1519, the Tallinn Administrative Court has found that personal data are rights and obligations related to the person of the bequeather. The court has clarified that upon interpretation of subsection 9 (2) of the Personal Data Protection Act, the provision must be understood as meaning that a person must first prove that they are the successor. This can be done with a succession certificate. The Inspectorate has previously said that if health data is needed earlier, it is possible to prove succession by applying for a declaration of acceptance of succession. This does not prove that the person will definitely become the successor of the property, but the notary will presumably check upon the submission of the application for succession that the person is entitled to succeed at all. The final assessment of which document is accepted as proof of the right of inheritance is made by the data processor (health care provider, the Health and Welfare Information Systems Centre, etc.). However, this is not the case in the light of the court decision, and the person must still have a real succession certificate in order to obtain the health data of the deceased.

WHY DID BUYING PRESCRIPTIONS FROM E-PHARMACIES FOR ANOTHER PERSON HAVE TO BE STOPPED?

The last day of November last year marks the decision to suspend the publication of the prescription information of another person in e-pharmacies, which showed how difficult it can be to find a solution if there are many parties in the process. No solution has yet been found at the time of publishing this yearbook, but the most important activities to date are described in this article.

At the end of November 2020, the Inspectorate discovered that in three e-pharmacies (apotheka.ee, sydameapteek.ee, and azeta.ee), it is possible for everyone to get acquainted with the prescriptions issued to another person by entering their personal identification code¹. The e-pharmacy required a login with an ID-card and the personal identification code of another person had to be entered, after which all of their outstanding prescriptions were immediately displayed. After that, it was possible to buy the prescription medicine or leave the e-pharmacy without making a purchase. However, the person to whom the

prescription was made did not have an overview of who had viewed their prescription information and when, because the Prescription Centre on the website www.eesti.ee only shows which pharmacy has viewed their data and when. This process did not establish in any way whether the user who logged in and viewed the prescriptions (health data) of another person had a legal basis (legal or authorised right of representation) to receive the prescription data.

In Internet banks, it would be unimaginable for it to be possible to view the current account statement of another person or make payments with their account simply by knowing their personal identification code. Prescription data are health data, i.e. special categories of personal data in accordance with the GDPR, which should be protected even more carefully.

The Inspectorate assessed the risk to data subjects as very high, which is why it exceptionally exercised the right granted under § 40 (3) 1) of the Administrative Procedure Act to issue an administrative act without hearing the objections of the participant in the proceeding. On 30

¹ The information displayed included the time of the prescription, the name of the prescriber, the prescription period, the active ingredient(s), and reference to the disease (or group of diseases) in which the medicine is used (e.g. anti-asthma medicinal products; acne products; other medicinal products for the nervous system; cardiovascular system; urogenital system, and sex hormones).

November 2020, the Inspectorate issued a precept with a 24-hour enforcement period to suspend the display of the list of valid prescriptions of a person in e-pharmacies to other persons on the basis of a personal identification code. The precepts were issued for OÜ Mustamäe Apteek, Veerenni Apteek, OÜ and OÜ PharmaMint.

To explain the reasons behind the decision, we must first give an overview of what the system is like today.

The participants in the prescription system are the patient, the doctor and the information system used by them the Health Information System (digilugu.ee, patient portal), the Prescription Centre, the pharmacy, and the information system of the pharmacy².

Description of the system

A system was set up years ago for buying a prescription on behalf of the person to whom the prescription was made, in accordance with which the doctor, when making the prescription, should determine the purchaser based on the expression of will of the patient. It is possible to choose between three options: the person to whom the prescription is made, i.e. the person themselves, a named third person, or an unspecified person. The second option, i.e. a named person, can only be realised if the patient has authorised a specific third person on the patient

² These are information systems used in the daily work of private health care providers, family doctor centres, and hospitals, from where the data are transferred to the central data set of the state – the Health Information System. The prescription data is forwarded to the Prescription Centre maintained by the Estonian Health Insurance Fund.

portal digilugu.ee. It is not possible to indicate the authorised persons appointed to purchase the prescription on the prescription itself. However, the system created years ago has not been implemented in practice. In the Prescription Centre, the default buyer of a prescription medicinal product from a pharmacy is an unspecified person. Neither the doctors nor the patients are aware of such a choice when making the prescription. Patients are also unaware of the possibility of authorising a third person on digilugu.ee.

Legal view

The health (including prescription) data of a person can be seen by themselves, their doctor, the pharmacist who is going to sell the medicinal product, and, with the authorisation or consent of the person, by a third person whom they send to the pharmacy to buy the medicinal product. Transactions on behalf of a child and an adult with restricted active legal capacity are performed by a legal representative, parent, or guardian.

The pharmacist must determine whether the person buying the medicinal product has the authorisation or right of representation of the patient. If the patient has previously appointed an authorised person on the patient portal and the doctor has prescribed the medicinal product with the option 'named person' or 'unspecified', the e-pharmacy can rely on the authorisation data displayed to the pharmacy from the patient portal and display/sell the medicinal product on the basis of the expression of will of the patient, which is clearly verifiable.

Immediately after the precept of the Inspectorate, the issue was also raised by the Social Affairs Committee of the Riigikogu and later by the Chancellor of Justice. The Inspectorate submitted proposals for solutions to the Ministry of Social Affairs:

- 1) the awareness of doctors, pharmacists, and people has to be raised so that the type of the person buying the medicinal product is chosen consciously, not by default, and so that people could use the patient portal to authorise third persons to buy their medicinal products;
- 2) the type of person buying the medicinal product could also be changed afterwards on the patient portal;
- 3) ideally, a person should be able to add authorised persons by prescription (not time-critical);
- 4) the doctor should be able to add authorised persons to the prescription (e.g. if the person does not use a computer and tells the doctor immediately who will buy it) and change the type of person buying the medicinal product;
- 5) the doctor should be able to determine for themselves, without the expression of will of the patient, the way in which the medicinal product is bought if they know that the patient is without capacity to exercise will;
- 6) inquiries to the population register should be used to create a way to verify the legal right of representation (minors, wards) which would be equally applicable in both regular and e-pharmacies;
- 7) prescription medicinal products can only be purchased in an e-pharmacy with a strong authentication tool for identification;
- 8) e-pharmacies should show the data subject the view logs of their prescriptions together with the personal identification code of the viewer;
- 9) to ensure the availability of medicinal products, digital and paper powers of attorney can also be used when purchasing medicinal products.

However, if no authorised person has been appointed on the patient portal, the person buying the medicinal product should prove the right of representation in another way. This is where the views of the parties differ. The managers of e-pharmacies found that in the case of a prescription with an unspecified buyer, the data subject has given consent (or the right of representation) for an unspecified group of persons to receive their special categories of personal data. In practice, however, the actual intention of the patient in regards to the buyer of the medicinal product has not been realised in any way – no one has determined it. Thus, it cannot be concluded that the patient has given their informed consent to the disclosure of their special categories of personal data to third persons in accordance with Article 9 (2) (a) and Article 7 of the GDPR.

The Inspectorate cannot accept that an e-pharmacy could trust anyone who claims to have the right of representation (or, moreover, bypass checking it by default). Coming back to the comparison with banking, it would mean that the bank would blindly trust anyone who walks into a bank branch and claims that they have the right to transfer money from an account of another person. In accordance with the GDPR, the pharmacy, as the controller, must ensure that it does not release special categories of personal data without a legal basis. In addition, the inspectorate found that the automatic display of all outstanding prescriptions was unnecessary.

During the procedure, it became clear that in some pharmacies, printouts of prescription lists were also issued to anyone who asked for them.

Handing over a printout of the list of prescriptions in a physical pharmacy to a person who only knows the personal identification code of another person is also a breach of law.

The interface with the population register could be done by the pharmacies themselves or by the Prescription Centre centrally. These three e-pharmacies did not want to develop the interface, but expect it from the state. The Health and Welfare Information Systems Centre has replied to the Chancellor of Justice that they have the readiness for the developments, provided that the Health Insurance

Fund and the Ministry of Social Affairs provide specific development needs. The Health Insurance Fund gave the Chancellor of Justice a general answer – finding solutions requires the cooperation of several agencies. The State Agency of Medicines wrote in March 2021 that it is not probable in the coming months that the interfacing of the population register will become reality but the Health Insurance Fund is looking for solutions.

Four months after the precept was issued, the creating of the interface with the population register has not progressed at all. In other words, in the case of minors and persons with restricted active legal capacity, the legal right of representation (and in the case of children, the right of custody) cannot be verified with inquiries from the population register.

In 2020, 10,526,571 prescriptions were purchased. Of these, 2,430,212 were purchased for another person (23%). 16% of these other persons were minors.'

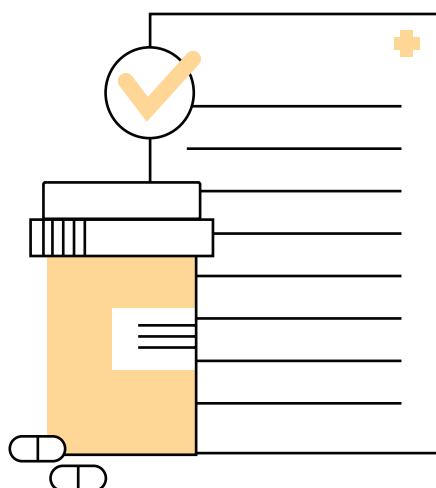
The interface with the population register would solve the situation regarding almost 400,000 prescriptions.

The three e-pharmacies operating on the market have proposed as their only solution that the pharmacist could ask control questions in order to check the right of representation. Unfortunately, all the proposed control questions still mean a risk. For example, it is not enough to know the name of a medicinal product or active substance, because the person buying the prescription can say the names of common medicinal products to see if the patient is taking any of them. They may also know that the patient has taken the medicinal product in the past. Knowing the name of the doctor who made the prescription would not be a good solution either because in rural areas, there is only one doctor in the village.

The Estonian Pharmacists' Association has submitted a proposal to the Ministry of Social Affairs to amend the law which wanted to legitimise doing nothing: if a prescription is issued with the choice of an 'unspecified buyer', the pharmacist does not have to check anything else.

Mustamäe Apteek OÜ (Apotheka) has also challenged the precept of the Inspectorate in court. The court proceedings are pending.

So, at the time of writing, the situation is still bleak. Unfortunately, the Inspectorate cannot instruct e-pharmacies or the state to develop the interface to the population register or make some other necessary development. However, a new type of e-pharmacy entering the market seems to take the need to create a secure solution seriously.



COMPLIANCE WITH THE PUBLIC INFORMATION ACT

People have a right to know what public authorities do on a daily basis – what policies are followed, what laws and regulations are being prepared, what programmes and projects are underway, how public money is being used, and what international agreements are being negotiated.

The purpose of the Public Information Act is to ensure the public nature and possibility of everyone to access information intended for general use, based on the principles of a democratic and social state governed by the rule of law and open society, and to create opportunities for public control over the performance of public tasks.

Access to public information is important so that people can participate in public life. Without access to public information, opinions cannot be formed or discussed.

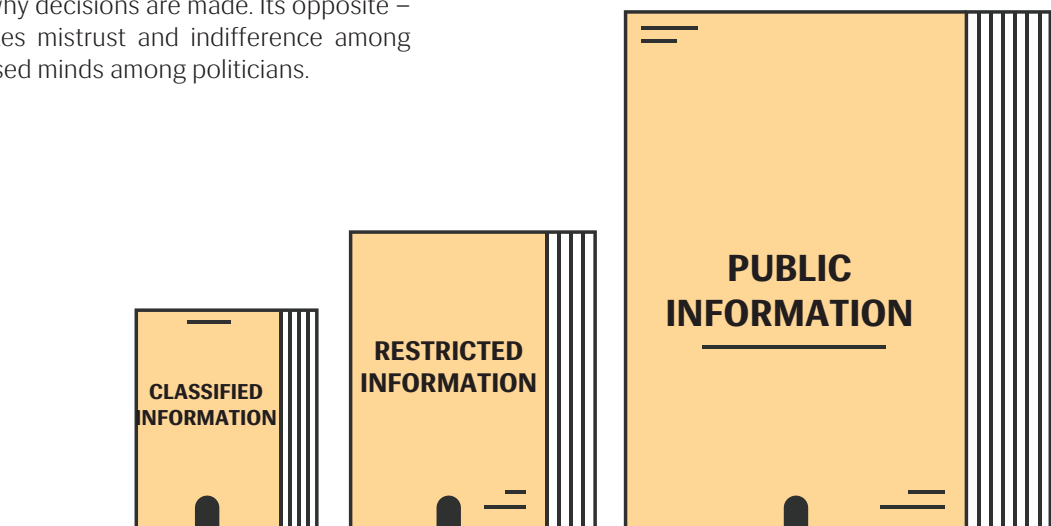
Access to information is also essential to ensure the openness and accessibility of public offices. It is also necessary to ensure that the state agencies work in the interests of society. The society can expect the government to provide access to at least some information that explains and justifies government policies and actions – for example, describe why the representatives of a state authority have decided to sell a state-owned company or explain and provide documentation on how a proposed waste facility will affect the environment.

Therefore, every person has the right to receive at least some information about decisions of public importance taken by public offices. Open and transparent decision-making is the basis of any democratic system, i.e. the citizens have the right to know how and why decisions are made. Its opposite – secrecy – creates mistrust and indifference among citizens and closed minds among politicians.

Availability of information

Both state agencies and local governments had problems in making public information available. When asking a public agency for public information that is generally available, the person requesting the information does not have to explain why they want the information. In practice, however, there are cases where the holder of the information has not complied with the request for information on the grounds that the requester has not given reasons for requesting the specific information. There have also been cases where the holder of information fails to comply with a request for information on the grounds that they consider that the requester does not need to know that information. In the case of public information to which there is no reason to restrict access, the holder of the information cannot decide on behalf of the person requesting the information or assess whether and why they need the information. The holder of information may refuse to comply with a request for information only if the information is subject to a restriction on access or a special procedure for accessing the information is prescribed in a specific law, in which case the specific law must be followed. However, care must be taken not to make restricted data public.

The modern digital age allows information to be quickly collected, processed, and disseminated. Once the data becomes public on the Internet, it is very difficult to slow its distribution. It is not enough for the publisher to remove it from the internet as it has already reached several or even tens of thousands of people who can process and distribute them. Therefore, when disclosing information, it is necessary to think thoroughly about what and how to disclose and what kind of data should be restricted.



The most frequently used basis for a restriction is clause 35 (1) 12) of the Public Information Act – information which contains personal data if enabling access to such information significantly breaches the inviolability of private life of the data subject.

A restriction is not always imposed for the name of each person, but the disclosure of such information must seriously infringe the privacy of the person.'

The Inspectorate agrees that any disclosure of personal data infringes the privacy of someone to some extent, but in order to impose a restriction, there must be a significant invasion. This is a discretionary decision that must always be assessed and, if necessary, justified. However, if a restriction were imposed on all documents containing the name of someone, a restriction on access could be imposed, in principle, to all documents, which is clearly not the intention of the above provision or of the legislator. As the above provision is a discretionary decision, the Inspectorate cannot decide on behalf of the state agencies on the need to impose a restriction.

The Inspectorate continued to receive questions as to whether a restriction should be imposed on any specific document. In such cases, the agency can only be advised on what should be considered or taken into account, but the final decision must still be made by the agency itself. However, in addition to the presence of the name of the person in the documents, the entire content of the letter must be assessed when the restriction is imposed. Even if the document does not contain the name of any person, but describes very precisely the location of an event and the persons who took part in the event, the persons may be identifiable by other information. Disclosure of such a document could seriously infringe on their privacy.

Document register

Questions have also been raised by the situation where the law does not allow the disclosure of data on natural persons in the public view of the document register, but there is no reason to impose a restriction on access to a document containing the name of a natural person. Here, it must be taken into account that it must be pos-

sible to perform full text searches using the search engine from the public view of the document register, which means that searches must be possible on the basis of all the metadata in the document register. If the name of a natural person recipient/sender were also public in the public view of the document register, then a single search would make it possible to get an overview of all inquiries submitted by that person and documents sent to them, which would make the person easily profilable. However, if you search for documents only by title, for example, to find out which documents are specific to a particular person, all those documents should be opened, and even then, you will only find out if that person has received/sent specific documents.

'Non-disclosure of the names of natural persons in the public view of the document register prevents the profiling of persons.'

However, the non-disclosure of the names of persons as data of the recipient/sender in the document register loses its effect if a private person is indicated as the recipient/sender but the name of the person is public in the title of the document. Such errors are found in documents concerning the social field, where the violation may be greater. This is mainly due to the fact that most officials register their documents themselves, but are not aware of which fields in the internal view of the document register are displayed in the public view of the document register or do not pay attention to it. The Inspectorate has repeatedly drawn the attention of holders of information to the problem in recent years.

Business secret

The second most frequently established basis for restriction has been clause 35 (1) 17) of the Public Information Act. This is information whose disclosure may violate a business secret. It is quite common for a contract concluded with legal persons in private law to include an obligation of confidentiality and, in the event of a request for information, to refuse to issue contracts on the grounds of it being a business secret. However, it should be noted that not all information can be a business secret of a company with a contract with a public sector body. A business secret has its own characteristics that it must meet. A com-

pany which concludes contracts with a public sector body or submits any documents to a public sector body must also take into account that the public sector body cannot agree with the company on the confidentiality of the information. A public sector body may restrict access to information only if there are legal grounds for doing so. For example, no contract can be fully covered by a business secret. The parties to the contract, the subject of the contract and, in the case of service contracts, the amount of the contract must always be public. If the contract also contains dispute settlement procedures, force majeure provisions, etc., such parts of the contract cannot be covered by business secrets either.

‘Quite often, the Inspectorate receives complaints that the request for information is not complied with on the grounds that the other party to the contract considers that all information is a business secret and that the holder of the information has not assessed at all whether and which documents include business secrets.’

CHALLENGE PROCEEDINGS

Last year, more appeals were lodged than usual against the decisions of the Inspectorate to close proceedings. The appellant was not satisfied with the termination of the proceedings and considered that the Inspectorate should issue a precept to the holder of information. It was striking that it was increasingly important for the appellants that the data processor be penalised. It is also often irrelevant whether or not data processing is terminated. For example, the Inspectorate had complaints where the Inspectorate had not satisfied the complaint of an appellant regarding the request for their data as this would have harmed the rights of other persons. The appellant considered that as the correspondence had been forwarded to the Inspectorate, the Inspectorate should forward it to them. The Inspectorate rejected the challenge on the grounds that the right to access one’s personal data is not absolute – the right of a person to receive data about themselves and the right of another person to freedom of opinion and privacy must be considered.

As a rule, such disputes end with a precept where the holder of the information must assess the existence and extent of the business secret in the requested documents.

Last year, the Inspectorate also had a case in which a person disclosing information declared the documents restricted information on the basis of clause 35 (1) 17) of the Public Information Act although the company found that not all documents contained business secrets. To avoid a situation where restrictions are imposed just in case, the Inspectorate recommends that before concluding contracts, the company be allowed to indicate what is considered a business secret in a document. Even if it is not possible to ask for this during the transmission of documents and a restriction has been imposed on the document, in case of a request for information, the holder of the information must still find out whether and which specific document contains a business secret. If necessary, the other party should be asked for explanations.

Last year, there was a surprising amount of people who were confused as to when a request for information is made in the sense of public information and in which case is it a request for information made about oneself within the meaning of the GDPR. This did not cause any problems before the entry into force of the GDPR because in both cases, the deadline for replying to a request was five working days. However, after the entry into force of the GDPR, the request for information about a specific person must be answered within one month. In several cases, a complaint was filed after five working days had passed since the person asked for their data.

‘If the release of data concerning the person submitting the challenge may infringe the rights of other persons, the data concerning them will not be released to the person (Article 15 (4) of the GDPR).’

In addition, the Inspectorate does not ask the agencies for data about the appellant or pass it on to the appellant. The Inspectorate checks the lawfulness of the refusal to issue data and, if a violation is established, obliges the agency to release the data.

RESPONDING TO REQUESTS FOR INFORMATION

The number of citizens who submit a large number of requests for information to agencies has increased year by year, and if they do not receive a reply in time or are not happy with the reply, they submit a challenge to the Inspectorate. Everyone has the right to request information but when it becomes their 'full-time job', the question arises as to whether it was the intention of the legislator to enable people to request information in this way. Notwithstanding the above, the holder of the information is obliged to respond to requests for information. To this end, it is always necessary to assess what the person making the request for information has requested in their request for information and whether it is a request for information or a request for explanation.

In accordance with subsection 23 (3) of the Public Information Act, if the holder of information refuses to comply with the request for information, it must also be substantiated. Therefore, a refusal cannot be considered justified if the holder of the information refuses to comply with the request for information on the grounds that access to the information is subject to restrictions. Situations like this are quite common – the holders of information do not bother to assess whether and to what extent the document is subject to restrictions. However, the holders of information may refuse to release information only if there are legal grounds for refusal.

The fact that the documents contain some restricted information does not mean that the documents will not be issued upon a request for information. In such a case, the part of the information or document to which the restrictions do not apply must be issued (subsection 38 (2) of the Public Information Act).'

Another common violation is failure to respond to requests for information on time. If a citizen has titled their request 'Request for information', but the request is actually a request for explanation, the request must be answered within five working days. The holder of information can refuse to comply with the request for information by clarifying that it is a request for explanation. The citizen does not need to know when their request is for explanation and when it is a request for information. The holder of the information, however, has to know this. Although the above problem has been discussed for years, it continued to be the biggest reason for submitting challenges.

Last year, there were also a number of cases where a person making a request for information addressed their request for information to a specific official and demanded that that official reply to them. As the holder of the information is the agency and not its employees, the person making the request for information cannot expect to get a reply from the official to whom they made the request for information. Such a request for information to a specific official may also mean that the request for information is not replied to within the time limit. This is because, for example, the person may be on holiday or ill or have missed the request for information. If a request for information has not been sent to the general email address of the agency, the agency cannot guarantee that the request for information will be answered in time. This does not mean that requests for information should not be sent to the email address of officials, but it is advisable to also send it to the general email address of the agency.

MONITORING LOCAL GOVERNMENTS

Last year, the Inspectorate carried out another monitoring to review the websites and registers of documents of local governments and to identify shortcomings. The monitoring was carried out between 26 August and 21 September.

The aim was to monitor how local governments comply with the disclosure requirements set out in the Public Information Act. The choice of which disclosure of information to check was also based on which complaints have been filed, what has changed in the law, and what information could be important for the citizen to find. The aim was also to map the general situation of information disclosure in local governments.

In addition, the Inspectorate considered it necessary to assess the procedure in the document register regarding providing access to the documents and protecting information meant for internal use.

The monitoring focused on the following:

1. Can the data of the data protection officer be found on the website, in the commercial register?
2. Disclosure of data protection conditions.
3. Disclosure of public procurements, including the availability of the procurement plan and procurement procedure.
4. Disclosure of council legislation and minutes.
5. Disclosure of the budget.
6. Disclosure of staff directives (holiday, additional remuneration).
7. Availability of procedures for granting social benefits, including application forms.
8. Access to emails through the document register.
9. 'For internal use' notations in the document register and providing access to information meant for internal use.
10. Disclosure of the names of natural persons in the document register.

Because from 15 March 2019, clause 36 (1) 9) of the Public Information Act does not allow documents concerning the use of budgetary funds of the state, local governments, or legal persons in public law and remuneration and compensation paid from the budget to persons working under an employment contract to be classified as information for internal use, the monitoring looked at whether and how local governments publish directives for the holidays, as well as the payment of additional remuneration and bonuses.

The Inspectorate also randomly checked the disclosure of detailed plans, the correctness of metadata in the document register, and information on the accessibility of websites either in emergency situations or when a web visitor cannot consume the information in the usual sense.

Summary

In total, it was possible to get a maximum of 10 points. The maximum points were awarded to the Põlva rural municipality government for which no deficiencies were identified during the random inspection. Three rural municipalities received 9.75 points – the rural municipality governments of Mustvee, Põltsamaa, and Jõhvi. The local governments were also appointed colours in accordance with the results of the monitoring. Local governments with a score of 8 to 10 points were appointed the colour green, local governments with a score of 5 to 7.75 points were appointed the colour yellow, and local governments with less than five points were appointed the colour red. This time, no local governments were appointed the colour red. Out of 79 local governments, 42 local governments were appointed the colour green and 37 local governments the colour yellow.

The results of the monitoring are available at www.aki.ee.

CHALLENGES



Issuing the minutes of the packaging committee

The case is addressed in the yearbook because the agency did not issue to the person making a request for information the minutes that were intended for internal use.

More information about the case¹ is available at www.aki.ee, but in conclusion, the Inspectorate found that the failure to issue the minutes of the packaging committee is not sufficiently justified if the Ministry of the Environment (agency) restricts access by clause 35 (2) 3) of the Public Information Act – in justified cases, documents addressed to persons within the agency which are not registered in the document register (opinions, notices, memoranda, certificates, advice, etc.). The holder of information did not provide compelling reasons why it would be necessary to restrict access.

When issuing the records, the holder of the information can provide a corresponding explanation which should preclude the opinion that the committee has also made decisions with the records.

In addition, the person making the request for information was aware that these were advisory recommendations and wished to see where the Minister had taken the opinion of the advisory body into account. In some cases, it may be important that the public is also given access to the opinions and recommendations that influence the decision, which helps to make national decisions transparent and checkable to its citizens.

The Inspectorate required the agency to issue the minutes of the packaging committee.

Restriction on access to a draft document

In the precept-decision on challenge² issued to the Environment Agency, the Inspectorate found that the holder of the information had misinterpreted clause 35 (2) 2) of the Public Information Act.

The Environment Agency considered that the coordinates of the permanent observation plots are a draft document, as these data will continue to be used in the future. Coordinated observation plots are restricted information as they belong to a document

¹ No. 21-3/20/3918 I

² No. 21-3/20/3918 I

(a statistical forest inventory survey) before that document is adopted (based on the same data, statistical forest inventory surveys will be published in the future). In addition, the Environment Agency initially claimed that the locations of the temporary observation plot were also linked to the location of the permanent observation plots. This claim was later dropped.

By a precept, the Inspectorate obliged the holder of information to issue permanent inventories or find another legal basis for restricting their access. A restriction on access to a draft document can be imposed on a case-by-case basis, but this presupposes that the restriction only applies until the document has been adopted or signed, i.e. the final version of the document has been created that will no longer be changed. Thus, if the information requested is no longer in the process of being amended but is a final approved document, such a restriction cannot be used for the coordinates of all existing (1999–present) and future forest inventories.

Disclosure also means the extraction of existing information, regardless of the form or data medium in which the information is stored. This means that public information may also be on other data media and otherwise accessible.'

In this case, this meant the possibility of extracting the requested information through a corresponding request and does not presuppose that the information requested should already be available as a document in the form in which it is requested.

The Inspectorate found that the basis for restricting access to a draft document should primarily ensure that information at the draft stage is not actively disclosed, which would allow it to be widely distributed so that the recipient of the information can no longer be certain whether the information received is correct. However, this does not mean that the information could not be made available to interested parties upon request.

The Environment Agency made the locations of the temporary statistical forest inventory observation plots public.

Business secret

The Inspectorate received a challenge of interest to the public, where the Ministry of Finance refused to issue a contract between the Estonian state and the law firm Freeh Sporkin & Sullivan and its annexes to AS Ekspress Media due to a business secret.

The use of a business secret basis does not give grounds for refusing to disclose information, but the right to cover the part (sentences or parts of sentences) concerning the business secret in advance. The business secret must meet the conditions set out in subsection 5 (2) of the Restriction of Unfair Competition and Protection of Business Secrets Act.

The Inspectorate issued a decision on the challenge and a precept warning¹ stating that since the Ministry, as the holder of information, imposes restrictions on access to documents, it must also be able to assess and justify how disclosure of such information harms the business interests of the operator (if necessary, asking them for explanations). However, much of the information was released after the intervention of the Inspectorate, and the Ministry acknowledged that the proportion of information with restricted access was small.

¹ No. 21-3-20-2309

LEGISLATIVE DRAFTING DEVELOPMENTS

In 2020, the Inspectorate was asked for an opinion on draft legislation on many occasions. Almost all ministries sent proposed legislative changes to the Inspectorate. The Ministry of Social Affairs submitted the most drafts for an opinion. The Inspectorate also advised the Ministry of the Interior, the Ministry of Economic Affairs and Communications, the Ministry of Finance, Ministry of Justice, the Ministry of Education and Research, and the Ministry of the Environment.

The most popular topic the Inspectorate was contacted for was changes in legislation concerning databases, whether at the level of the law or the statutes. It can be said that most comments have had to be made about the data sets – why any data is collected and why such data. However, we also provided explanations on collection purposes and retention periods. The data sets tend to be too broad in relation to the purpose, and it is not clear how any of the data to be collected will help to achieve the purpose of the database or is consistent with it. With regard to retention periods, we had to point out that they were too long and that it is necessary to justify why such a retention period was intended. The overarching concern with the draft databases was the collection of data just in case.

Bottlenecks

Legislators are probably concerned that amending a piece of legislation, especially an act, is a long and complex process, which is why they want to anticipate as many situations as possible for the future. This causes the Inspectorate to wonder why it is desired to keep any data for so long or collect it at all. The answer is often not given in the explanatory memorandum either. It seems it is not always understood what the purpose is of clear provisions and the ability to justify their choices in the explanatory memorandum. The Inspectorate is obliged to ensure that legislators follow the basic principles of data protection in data processing – lawfulness, purpose limitation, transparency, and data minimisation. Legislation – be it acts or, in the case of databases, statutes – must give the person an answer as to what data about them is collected, why, and for what purpose. It sometimes seems that the legislators give explanations to them-

selves or, in rare cases, to other agencies that have to approve the document. The explanations are either too complicated or too brief, meaning that only those who are dedicated to the subject can understand them. However, the addressee is data subjects or people.

Data protection impact assessments also tend to be lacking or too brief. That is why we have had to point out the need to supplement the data protection impact assessment on several occasions. The impact on the privacy of people also tends to be assessed to be smaller than it often actually is.

Coordination of changes in data sets in the administration system for the state information system seems to continue to be a major problem.

In most cases when the change concerns the statutes of the database, the Inspectorate had to admit that the administration system for the state information system had not been updated.'

For example, the databases of the Health Information System, which was changed three times last year and is planned to be changed again in 2021, have not been approved in the administration system for the state information system since 2014. In addition to the above, there is often ambiguity of definitions – one time, one term is used, another time, another is used, without explaining what is meant by it. Once again, it can be seen that the people preparing the draft forget that the addressees of the legal act are regular people.

It has already been pointed out that it is often desired to store data for a very long time, and it is not possible to explain why such a retention period has been chosen. Another problem with the drafts was the fact that it was not stated what would happen to the data when the retention period expires – whether the data is deleted or stored in some other way, such as anonymised in an archive, and if so, for how long.

The foregoing summarised the observations on the drafts submitted to the Inspectorate for approval. Last year was clearly affected by the crisis caused by the COVID-19 virus, but it is now obvious that it will continue this year. As this is primarily a health care crisis, it had the greatest impact on health legislation – a number of shortcomings in the legal framework emerged. On the one hand, this is understandable, because many acts, such as the Emergency Act, had to be implemented for the first time and, as it turned out, it had not considered a crisis like the one that hit us in spring 2020. It is, on the one hand, understandable that shortcomings were discovered

in the regulation of the Health Information System, as well as in the Communicable Diseases Prevention and Control Act and in several other relevant legal acts. However, as an observer of legislative work, it can be said that these changes were made in a hurry and at times ill-considered.

The following is an overview of the drafts that the Inspectorate commented which were more publicly discussed or were more important or more influential from the point of view of the Inspectorate.

AMENDMENTS TO THE STATUTES OF THE HEALTH INFORMATION SYSTEM

As has already been said, the Ministry of Social Affairs had the busiest year for obvious reasons.

The first change to the Health Information System took place before the onset of the health crisis, and the most important change concerned the new data sets entered in the Health Information System. Namely, it had to be noted that as a result of the changes, the data set of treatment guides would also become one of the data sets in the central database, even though the corresponding provision of the Health Services Organisation Act (subsection 59³ (2¹)), which exhaustively defines the nature of the data that may be processed in the Health Information System, does not provide for such a data set. In addition, the Inspectorate drew attention to the issue of access to health data for the second time. Namely, one amendment concerned clauses 17 (1) 4) and 8) of the Statutes of the Health Information System which give the data subject the right to refuse and allow access to their data and to allow the viewing and modification of their data. We noted that the difference between the two described rights is difficult to understand. The Inspectorate also pointed out that we had already drawn attention to the issue of access to data in the Health Information System more broadly in December 2019. Article 9 (3) of the GDPR provides that where special categories of personal data are processed for the purposes referred to in Article 9 (2) (h) (preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or

the management of health or social care systems and services), the employee of the data processor must be subject to the obligation of professional secrecy under Union or Member State law. Subsection 59³ (2¹) of the Health Services Organisation Act specifies which persons participating in health services also have access to the Health Information System.

However, they probably do not all have a legal obligation to maintain secrecy. Thus, the new amendment that allows a person to manage access may lead to a situation where data is accessed by someone who is not bound by professional secrecy. In addition, the Inspectorate pointed out for the second time that one of the data providers to the Health Information System is the Ministry of Education and Research, which transmits to the Health Information System the data of students, data on their level of education, and data on their educational institution. The fact that the need and purpose of collecting such data is not clear was already pointed out in 2018.

The HOIA application

The next amendment in the Health Information System mainly concerned the creation of the HOIA application.

First, the Inspectorate pointed out that the data exchange between the Health Information System and the central server of the application should take place over the X-tee.

The second observation concerned the transmission of codes. The process was confusing – which code was sent where and when? The use of the definitions ‘verification code’ and ‘identification code’ and, in some cases, ‘anonymous code’ was ambiguous. Thus, it remained unclear whether these were synonyms or different codes. The explanatory memorandum did not answer these questions. It turned out that the data exchange is designed in such a way that the confirmation code is created in the application, from where it is transmitted by the user to the Health Information System. If the confirmation process in the Health Information System reveals that the health documents of the person identified in the information system confirm the diagnosis, an identification code is created. Then, both the confirmation code and the identification code are transmitted to the server of the application, and only the confirmation code is transmitted to the user of the application. The Inspectorate noted that if the anonymous code, which was partly used, is different from the confirmation code, the definitions must be clarified. In addition, the Inspectorate pointed out that the data protection impact assessment focused too much on the technical side and on the code exchange, i.e. data exchange in the application. Indirect risks were ignored and not assessed. In other words, if you have received confirmation that you have been in the same room with an infected person, is it possible to identify, even indirectly, who that person was? The risk of the application sending false positives was also not assessed sufficiently. Is it possible, for example, that two phones that have been close to each other for a long time due to the thin walls of an apartment building can exchange data and thus send a notification that you have been in the same room as an infected person even though you have not? In addition, if a person attended a meeting with just a few people and later were sent a notification that they have been in a room with an infected person, would they not be able to identify that person?

The explanatory memorandum said that the application does not process personal data itself. However, the Inspectorate pointed out that this may not be the case. Namely, if there is any possibility that the application processes even pseudonymous data, including if the identification of a person may be possible, even indirectly, thanks to the application, but also without it, all data protection requirements must be applied.

In addition, it had to be pointed out that although the identification code in the application and the verification code generated in the Health Information System are presumably unique, it could be understood from the explanatory memorandum that the verification code of the Health Information System is generated from the data of the Health

Information System. However, logs are created in the Health Information System for any data processing, which in turn means that information (identification code and log) is created in the information system, on the basis of which it is possible to identify the user of the application and the verification code used by the application. Thus, it can be said that the data processing is not completely anonymous.

Our recommendation was to give a clear overview of data processing to the users of the application, including in its user conditions.’

The most important thing about the third amendment to the Health Information System was the addition of subsection 1¹ to section 5, in accordance with which the owner of ambulance crew interfaced with the alarm centre transmits the data of the ambulance station and ambulance crew to the information system immediately after a change in the status of the relevant resource. According to the Inspectorate, the purposes of maintaining the information system do not allow the transmission of such data to the Health Information System. Although the explanatory memorandum indicated that the same data (resource data) is part of the ambulance card under current law, the data of which is transmitted to the Health Information System, but this is not a comparable situation. Namely, the ambulance card is designed to provide information about the health service provided and, although it also contains information about the ambulance crew that provided the service, the purpose of the ambulance card is not to manage the use of ambulances as a resource. In addition, it was not clear from the draft which data would be transmitted to the Health Information System by the owner of the ambulance crew interfaced with the alarm centre. As can be seen from the current Statutes of the Health Information System, this amendment has been abandoned.

The Inspectorate also had a comment on the transmission to the Health Information System of the data collected by the alarm centre during the processing of emergency calls made to emergency medical care. Attention had to be drawn to whether, in view of the principles of data minimisation and purposefulness of data processing, it is necessary to transmit all the data mentioned in the draft to the Health Information System, taking into account the purposes of maintaining the Health Information System.

Although the data in the Health Information System had not been updated in the administration system for the state information system since 2014, this was done immediately before the completion of this overview. Unfortunately, the data composition uploaded to

¹ Subsection 591 (4) of the Health Services Organisation Act

administration system for the state information system included a lot of data that is not covered by the Statutes of the Health Information System. It should be noted that the Health Services Organisation Act, which is the basis of the Health Information System, provides only a general definition of what data is collected in the Health Information System. The Statutes of the Health Information System also do not provide a detailed list of data. To find out what data is entered into the Health Information System, many different rules and legislations must be examined. However, no norm prescribes that the citizenship of the person, the time they settled in Estonia, or the data of their spouse be entered in the Health Information System. In accordance with the data set uploaded to the administration system for the state information system, the personal identification code of the person who purchased the prescription medicinal product from the pharmacy is also submitted to the Health Information System. However, the patient does not see this information in the patient portal and the statutes do not provide for the entry of this data in the Health Information System. The same

thing happened with the person who made the emergency call – the data composition revealed that the information is transmitted from the alarm centre to the Health Information System. There were other such discrepancies between the legislation and the reality¹.

In conclusion, the primary goal of the Health Information System is to be a central database for the provision of high-quality health services to people by providing the doctor with a comprehensive overview of the health data of the patient.

Unfortunately, the Health Information System contains more and more data that is not related to the provision of health services. One of the most important requirements of the Estonian state information system is dispersion. In other words, instead of one large database, there are many topic-based databases in Estonia that exchange the necessary data. Care must therefore be taken to ensure that the Health Information System does not become a database in which, in addition to health data of the person, half of their life history is collected.

THE DRAFTS PREPARED BY THE MINISTRY OF THE INTERIOR

We will focus on two of the draft legislation submitted by the Ministry of the Interior – the police database (POLIS), on which the Inspectorate was consulted twice, and the draft amendment to the Identity Documents Act and other acts, establishing the automatic biometric identification system database (ABIS).

Draft amendment to the police database

The changes to POLIS were mainly related to the COVID-19 crisis. The first change was sent to us in April and the second in June. Namely, the Health Board needed the help of the Police and Border Guard Board to check that both infected persons and their close contacts who had been assigned to quarantine are complying with the restrictions imposed on them. However, it turned out that the exchange of data between the different databases was not possible without changing the legislation.

The purpose of the amendment submitted in April was to create a legal basis for the submission of data by the Health Board to POLIS. In accordance with the draft, the Health Board would transfer data to POLIS to the data set of common information objects, preventive activities, and searches.

The Inspectorate first pointed out that although the draft stated that the right of the Health Board to transmit data from the Communicable Diseases Registry to the Police and Border Guard Board arises from subsection 11 (11) of the Statutes of the Communicable Diseases Registry, the provision actually provided a legal basis for access to the Communicable Diseases Registry and not for the transfer of data. In addition, subsection 22 (2) of the Statutes of POLIS does not allow the entry in the POLIS of a number of data, including data on the health status and sexual life of persons, except for the prevention, deterrence, and detection of a crime or the apprehension of a fugitive. Compliance with the quarantine requirements of a COVID-19 infected person clearly does not fall into any of these categories.

¹See 13 April 2021 No. 2.2.-8/21/879 'Non-coordination of the health information system'

The Inspectorate also drew attention to the deadlines for data retention. Namely, it was stipulated how long the data of the Health Board would be kept active, but it remained unclear what would happen to it after that. It would presumably be entered in the archives, but this was not explicitly stated. In addition, it had to be noted that even if the data is transferred to the archives, section 25 of the Statutes of POLIS provides for access rights to the archives, stating that in addition to the data subject, police officers and other people have the right to receive data from the archives if there is a justified need for them. However, the data protection impact assessment did not analyse the risk that a police officer or other person may also have access to the data of a person diagnosed with COVID-19. The data protection impact assessment was also incomplete as regards the access of other agencies to POLIS and thus to the data transmitted by the Health Board. Namely, subsection 19 (2) of the Statutes of POLIS provides who, in addition to the Police and Border Guard Board, has access to POLIS.

The amendment to the Statutes of POLIS made in June was similar to the previous one, which had already raised questions. As the April draft already introduced changes to POLIS which limited the Health Board as the person submitting data only in relation to the emergency situation declared in spring 2020, the new draft sought to establish a provision making the Health Board the person submitting data to POLIS in an emergency, a state of emergency, and a state of war – and not only during the emergency situation in spring 2020.

The Inspectorate pointed out that while the previous draft of the Statutes of POLIS was understandable in that the data transfer was related to the prevention of the spread of communicable diseases, the new draft did not make it possible to understand in which cases the Health Board would be obliged to forward data to the Police and Border Guard Board. Namely, an emergency may be declared for very different reasons, and it was not clear whether the data transfer would take place in any emergency. It was also unclear if and why and what data would be transmitted by the Health Board during a state of emergency and a state of war.

Once again, questions arose about the retention of data. As the explanatory memorandum clarified that it is organisationally possible to ensure that data is only retained until a certain event, this should be explicitly stated in the draft. Namely, the reluctance or impossibility to create a new IT solution was pointed out as the reason why the retention periods cannot be set more precisely, but it was confirmed that a shorter retention period could be ensured organisationally. It was also not clear on what basis the proposed retention periods were assessed as appropriate and purposeful.

Like the previous time, the Inspectorate once again commented on the deadlines for preservation in the archives – in some cases, the deadline was as much as 50 years, but there was no explanation as to why such a deadline had been chosen. As other agencies also have access to POLIS data, the effects on the data subject had been assessed and it was found that the interference was not significant, which we did not agree with. Not all such agencies that have access to POLIS in an emergency, a state of emergency, or a state of war are given tasks that would justify access to the data transmitted by the Health Board. The explanatory memorandum was brief in this respect and focused on describing the need to combat the virus, while the change would affect the rights of the Health Board in the future. In addition, the situations in which the Health Board should transmit data were expanded on the one hand, but unspecified on the other.

However, taking into account the current regulation of POLIS, it must be acknowledged that the proposed change was not implemented.

Establishment of an automatic biometric identification system (ABIS) database

One of the most important drafts of the Ministry of the Interior in 2020 was the draft amendment to the Identity Documents Act and other acts, creating a legal basis for the creation of an automatic biometric identification system (ABIS) database.

The Ministry of the Interior explains on its website that the database of the automatic biometric identification system will be the central national database where biometric personal data (facial images and fingerprints) collected in various data-

bases and within the framework of various national procedures will be stored. The purpose of creating the ABIS database is to contribute to secure identity management, more effective public order and security, crime prevention, and the gathering of evidence in criminal proceedings. ABIS helps to increase the reliability of identification and identity verification by providing an even better level of assurance that a person can have only one identity in Estonia³.

The Inspectorate pointed out⁴ that biometrics are special categories of personal data within the meaning of Article 9 (1) of the GDPR and their processing is generally prohibited. The processing of such data is permitted only if the legal basis for the processing of data complies with Article 9 (2) of the GDPR or, in the case of data processing for law enforcement purposes, with section 20 of the Personal Data Protection Act. In both cases, the legislation must allow for the corresponding processing of personal data.

It was important to emphasise that identification on the basis of biometric data, i.e. a special category of data, cannot become the rule – identification by the so-called conventional method must be preferred. As the draft amends not only the Identity Documents Act but also a very large number of other acts (14 different acts)⁵, the Inspectorate indicated that in cases covered by the amendment, identity must first be established by comparing the photo in the identity document with the person. If this is not enough, additional measures should be taken. If, in the circumstances, it is proportionate and necessary to use biometrics immediately, such processing should be an exception and the reasons justifying the exception must be derived from the law or at least from the explanatory memorandum. In addition, the

Inspectorate pointed out that subsection 116 (1) of the Identity Documents Act stipulates that the collection and processing of biometric data takes place with the consent of the applicant for the document. In such a situation, however, the person is not giving their consent within the meaning of the GDPR. Consent must be voluntary, revocable, and not dependent on consideration. If a person applies for an identity document on which biometric data are also entered and without which it is not possible to create the document, it is not possible to speak of data processing on the basis of consent. Such a situation therefore requires a clear legal basis.

Another important aspect was that the draft provided for provisions in which cases it is possible to process biometrics for identification in essentially undefined cases and situations (subsection 155 (6–8) of the Identity Documents Act). Chapter 5 of the Statutes of the ABIS also describes in which cases one-to-one (1 : 1) and in which case one-to-many (1 : n) queries are made, i.e. against most of the data entered in the ABIS. This, in turn, means that the data entered in ABIS will be used for a purpose other than that for which it was originally collected. However, as a general rule, data may only be used for the purposes for which it was originally collected (Article 5 (1) (b) of the GDPR). The Inspectorate also drew attention to the fact that allowing the processing of biometric data for secondary purposes must not be done carelessly. It must be foreseeable and clear to the person whose data are being processed that the data collected about them may also be used for other purposes and what those purposes are.

Although the explanatory memorandum to the draft was supplemented in this respect, it was maintained that processing for secondary purposes was necessary and in line with the GDPR. The explanatory memorandum explains that the draft provides the legal basis for the further processing of data which is necessary to ensure public order and security and covers the general purpose of the database to be created. The draft provides for the processing of data for a purpose different from the original purpose of

³ See also <https://www.siseministeerium.ee/et/eesmark-tegevused/automaatse-biomeetritili-se-isikutuvastuse-susteemi-andmekogu-ehk-abis>

⁴ The observations concern the version of the draft submitted to the Inspectorate, not the one the Riigikogu is discussing in spring 2021.

⁵ See also <https://www.riigikogu.ee/tegevus/eelnoud/eelnouf8b47e-e45f-43c2-8189-6bb875bf51fc/lsikut%20t%C3%B5endavate%20dokumentide%20seaduse%20muutmi-se%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus>

their collection primarily in identifying a person, i.e. in a situation where the identity of a person is not known to a public authority. The possibility to use biometric data collected in another public procedure, if necessary, is very important in identifying a person, because in the course of this, the identity of the person must be established. When identifying a person, the competent authority must verify, on the basis of various data and, where appropriate, biometric data and following extensive inquiries, that the person is who they claim to be. Public authorities have a legal obligation to identify a person and the right and obligation to act only in relation to the right

person. Therefore, public authorities must be convinced that the person is who they say they are. The right to take and process biometric data from a person to identify and verify their identity is provided for in the applicable law. For the Inspectorate, the biggest concern was whether the regulation would be sufficiently clear for people. In other words, is it clear, understandable, and foreseeable to any person that if their biometric data are used for their identification, then the data may in fact also be used for other purposes in some other situation?

OTHER DRAFTS THE INSPECTORATE PROVIDED ITS OPINION ON

The most important drafts or legislative intents sent to the Inspectorate by other ministries were:

- **The draft Tourism Act**
- **Legislative intent to develop the Credit Information Act**

The draft Tourism Act

The amendment to the Tourism Act regarding data protection was explained in the explanatory memorandum as follows: the draft provides for the electronic registration of accommodation service users and the processing of their data. The aim is to make it faster and easier for visitors and accommodation providers to comply with the visitor registration requirements of the Schengen Convention and to ensure better protection of the personal data of the visitors while ensuring that Estonia remains a safe and secure place for both locals and visitors. The data on accommodation users is also needed to compile national statistics and analyse tourism development and marketing.

Article 45 (1) (b) of the Schengen Convention states that the Contracting Parties undertake to adopt the necessary measures to ensure that the completed registration forms will be kept for the competent authorities or forwarded to them where such authorities deem this necessary for the prevention of threats, for criminal investigations, or for clarifying the circumstances of missing persons or accident victims, save where national law provides otherwise.

The Inspectorate drew the attention of the legislator to the fact that it is not clear from the wording of the Convention whether data is transmitted automatically, i.e. by the push method, or may be transmitted only if the law enforcement authority requests information by inquiry, i.e. by the pull method. The explanatory memorandum said that many European Union countries have chosen the push method, but there was no analysis of why Estonia has chosen the same path and whether the same goal could be achieved with the pull method. Therefore, the Inspectorate considered that preference should be given to the transmission of data by the pull method, as it is wrong to assume that the majority of people visiting accommodation establishments could ever meet such criteria to justify the automatic transmission of this data to law enforcement authorities. Push data transmission is certainly more intrusive on the privacy of the individuals.

The draft plans to implement electronic registration of accommodation service users in accommodation establishments and to simplify this, it is planned to start capturing data directly from the machine-readable code on the ID-card or passport. In its opinion, the Inspectorate indicated that the machine-readable code of identity documents includes much more data than is necessary for the accommodation service provider to collect. In addition, the more time passes, the more it can contain code data, including biometric data, for example. Therefore, the system should be designed in such a way that the machine-readable code is only used to collect the data set that the accommodation provider has to collect. It also had to be emphasised that any electronic solution that transmits data to a national database must do so via the X-tee.

In connection with the amendments to the Tourism Act, it was also planned to amend the Police and Border Guard Act. A legal basis will be added to the Police and Border Guard Act for the creation of an accommodation service user database, which, in turn, is a sub-database of the passenger name record database, into which the data of the accommodation service user specified in subsection 24 (1) of the Tourism Act is entered. As a result of the amendment to the act, the data of the person entered in the database of the accommodation service user will automatically be cross-checked against those databases and watch lists that are important for achieving the purpose of data processing. Only the data of the visitor whose data give a hit during the cross-check are manually checked so that the procedural authority can decide on the necessary action. The above explanation was only included in the explanatory memorandum. However, such information should be included in the act itself.

Attention was paid to the issue of retention periods. Namely, although it was said that the data of the user of the accommodation service will be pseudonymised six months after being entered into the database, it was not clear whether and how the data of persons whose data were not cross-checked were retained.

The Inspectorate recommended that the data of such persons should immediately be pseudonymised.'

The draft provided that in certain cases, the pseudonymised data could be re-personalised, but it was not clear how this would be done. The Inspectorate recommended regulating exactly under what conditions this is allowed. The Inspectorate also pointed out that although personal data is pseudonymised, the type and number of the travel document remain visible, meaning that the Police and Border Guard Board, for example, can identify the person due to the information in their possession, which may mean that the data is not actually pseudonymised.

There were also comments on the issue of access – the right of access had been granted to the Police and Border Guard Board and national security authorities. As the definition of security authorities is broad and derives from the Security Authorities Act, access to data is also granted to, for example, the Foreign Intelligence Service. As the need for access by the Foreign Intelligence Service was not explained in the explanatory memorandum, it remained unclear. The Inspectorate therefore recommended naming the authorities with access rights and justifying the need for access in the explanatory memorandum. We also had to point out the need to supplement the data protection impact assessment, both as regards to this and the processing of pseudonymous data.

Legislative intent to develop the Credit Information Act

The purpose of developing the Credit Information Act is noble and certainly necessary. The introduction to the legislative intent⁶ describes the need for credit information as follows: *the main purpose of the legislative intent to develop the draft Credit Information Act is to ensure more effective compliance with the principles of responsible lending by addressing two main topics: (a) the introduction of the Credit Information Act, i.e. the establishment of operational requirements and supervision for undertakings engaged in the brokerage of data on the financial liabilities of natural persons; (b) the obligation of credit providers to start sharing data on the financial liabilities of individual loan applicants.*

The legislative intent identifies a registry-based data exchange platform and the hybrid of the two as possible technical tools for exchanging information. Three solutions are proposed for the organisation of the data exchange: a national system where the register is maintained and managed by state agencies (1), a national system where the register is outsourced to the private sector (2), and a system that meets national conditions but is organised by the private sector, in which market participants themselves create the organisational and technical capacity to organise the exchange of data (3). The draft clearly favours the third solution.

The Inspectorate expressed the view that it is not necessary to create a new database or register for each new data processing. The solution of a data exchange platform should be preferred to concentrating data in one register or database.'

In the Estonian public sector, distributed database systems have been implemented for security reasons for many years. In the case of a request-based data exchange, the data issuer has a better opportunity to assess whether the request is justified.

The legislative intent stipulates that it must be mandatory for credit providers to transmit data and make requests. However, at least at this stage, it is not clear whether such an obligation would arise in the case of any application for credit or whether, for example, information on existing obligations would also be included in the system to be set up. In other words, whether the new system will have a prospective or retrospective effect. Presumably the latter, which, in turn, means that data is also collected on all those persons and their liabilities who may never want to make any financial commitments again. This means a great risk of collecting data just in case and creating a database despite the original noble purposes of it being available only to credit providers. There may also be a great deal of interest in other people gaining access to such a database.

For example, the Credit Register was originally established by private companies (banks) for the purpose of fulfilling the obligation to lend responsibly. Over time, however, the Credit Register became independent and issues payment default data to anyone who claims to have a legitimate interest in the debt data. If a so-called positive credit register is created, it is clear that it is possible for other interested parties to obtain data from the database if they have a legitimate interest in it. Therefore, even if the register or database is limited to creditors and other persons provided by law, it is essentially impossible to exclude the provision of data from it in the event of legitimate interest. The existence of legitimate interest must be assessed by the controller, but we can say from our practice that no one in Estonia is really able to do it. For this reason, the legislator must understand and make it clear to the public that when a new central database containing loan commitments is created, all sorts of other persons can also use this data for purposes that are currently unforeseen.

In addition, it would clearly not be purposeful to collect all existing loans in a central register 'just in case'. After all, the need to process data arises only at the moment of asking for a new loan. Many people who already taken a home loan may not want more loans at all or for many years to come. The collection of the credit data of such people in the register just in case and keeping it there for years or decades (and, as stated above, for other

⁶ väljatöötamiskavatsus ja vastust sellele on registreeritud kirja numbriga 1.2.-4/20/3366

purposes) has nothing to do with the purpose for which the register is intended to be set up.

The legislative intent proposes that consideration should be given to making licensed credit bureaus mandatory for creditors, unless the creditors themselves consider their measures to be adequate. Here, the question first arose as to why the creditor should use credit bureaus at all as it is possible that the creditor considers their measures to be sufficient. At the same time, they should provide the data to the credit bureau. The risk that credit bureaus collect data (because their submission is mandatory for the creditor in accordance with the law to be created) but do not use them is even more important. This may

give credit bureaus an economic interest in using this data for other purposes. The proposed amendment to the Law of Obligations Act mentioned in the legislative intent suggests that the proposed Credit Information Act is based on the assumption that both (central) registers and data exchange platforms will emerge that should be used to comply with responsible lending. Thus, the scenario feared by the Inspectorate is rather likely. It was only a legislative intent, but the Inspectorate hopes that this feedback has made the drafters think about important data protection aspects. The Inspectorate will naturally keep a close eye on the developments.

DATABASES PROCESSED IN THE ADMINISTRATION SYSTEM FOR THE STATE INFORMATION SYSTEM

The yearbook discusses the intention to establish two new databases.

- **Data collection register of the European Social Fund**
- **Information system of Tallinn Social Welfare**

Data collection register of the European Social Fund

In the case of projects financed by the structural funds of the European Union, the participants must be registered and kept until the end of the reporting and control period of the project. The State Support Services Centre wanted to establish a database for personal data collected within the framework of activities financed by the European Social Fund.

The structural funds of the European Union (at least the European Social Fund) fund many sensitive services (e.g. the homeless, those excluded from the housing market, adoptive parents; psychological assistance may also be a service). There has been a problem for services

funded in this way – data is collected from the participants without them knowing how many agencies (service provider, management authority, implementing agency, certifying body, audit authority) will subsequently process their data and for how long. Or, conversely, that a person is asked for their consent to the processing of data, but if they refuse, they will not be provided the service. Unfortunately, in such a case, consent can in no way be the basis for the processing of data.

The consent to the processing of personal data must be left to the discretion of individual without there being negative consequences. In this situation, it would be right to give the person a clear overview of the mandatory data processing accompanying a service financed by the structural funds, e.g. through a clearly worded leaflet, but without asking for their consent.

However, returning to the plan to establish a data collection register, the first problem in this case was the transmission of data as a copy to Statistics Estonia. The problem was that the data would be transmitted to Statistics Estonia as the processor of the Ministry of Finance in such a way that a real-time copy of the database of the Ministry of Finance would be created for Statistics Estonia. Although the Ministry of Finance has transferred its reporting task to Statistics Estonia through a co-operation agreement, it would be correct to give Statistics Estonia access to the database, rather than creating a real-time copy of the database.

Another problem was the transfer of the task and the use of the data of Statistics Estonia. Until now, these reports were considered statistical work outside the program, but the Inspectorate doubts whether this is true. In essence, the Ministry of Finance has authorised Statistics Estonia to perform its administrative task under a co-operation agreement. This is not statistical work in nature, but reports prepared for the purpose of monitoring the use of European funds. It would be completely unacceptable for such reports to result in a person being reclaimed.

The use of data from the so-called statistical registers of Statistics Estonia for making decisions with legal consequences for a person is completely prohibited.'

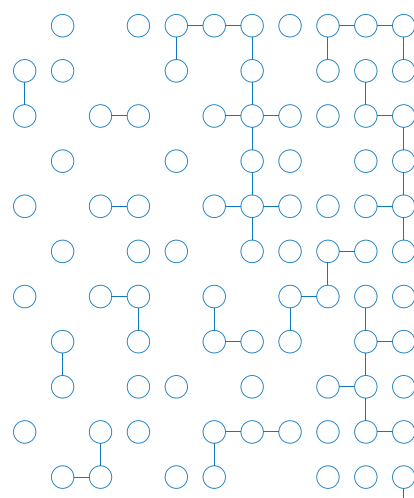
The Inspectorate considered that the whole concept of data processing should be rethought.

Information system of Tallinn Social Welfare

The establishment of a new database meant the issue of duplicate databases. Namely, about ten years ago, each local government had its own information system for organising social welfare (mostly SIUTS). The state considered that it would be right to establish the central state database STAR – a data register of social services and benefits – for the social welfare data of local governments.

The data set of STAR is enormous – it includes all data on all kinds of state and local government social services and benefits, as well as those wishing to adopt and adoptions. Last year, however, we ended up in the pre-STAR situation – the city of Tallinn created its own information system for the same reason on the grounds that STAR does not have the necessary functionalities for the local government. As the creation of two different databases for the same task is not justified in any way, the Inspectorate asked the City of Tallinn and the Ministry of Social Affairs together with the National Social Insurance Board to clarify which data is needed only by the local government and which by the state. The aim is to find out what the state should collect centrally and for what purpose. The right to supervise alone is not a sufficient reason to collect data by the state. For supervisory purposes, the National Social Insurance Board can request data from the local government database (or be provided temporary access) at any time. It must also be taken into account that social welfare is diverse: social welfare provided by the state itself, mandatory services imposed by the state on local governments, and voluntary services provided by local governments.

The Inspectorate is still waiting for an overview of the reasons for collecting STAR data from the Ministry of Social Affairs.



DATABASES OF LOCAL GOVERNMENTS

Unfortunately, the poor quality of the statutes became apparent in the case of databases of local governments. Statutes are copied from others, without understanding what its provisions mean or whether they correspond to reality. One of the most striking problems is the databases of hobby education of local governments. They include data on all hobby groups operating in the territory of the local government and the children participating in them – which child attended which hobby group and on what date. This is justified by the need to control the granting of support: although support is given to the organiser of the hobby group and not to a specific child, the aim is to check that the number of participants in the hobby group is in line with reality and that the same child is not registered in several groups. However, one local government wanted to identify children who do not attend any hobby group on the basis of the register. Attending a hobby group is not obligatory and does not mean that the child is in need of help. The local government should identify children in need in other ways.

The collection of personalised data for the purpose of verifying the circumstances of the payment of the support to the organiser of the hobby group should be kept to a minimum. For example, the necessary checks could be carried out automatically on a monthly basis and then the data could be anonymised, which means that all identifiable data would be destroyed. Keeping such data for years is not justified.

We still expect the City of Tallinn to bring the statutes of the pet register in line with the data collected in the register. At present, the statutes provide only for the collection of data on dogs (and their owners).

Some general observations

Pursuant to section 43⁵ of the Public Information Act, in addition to the data composition, the persons submitting data must also be indicated in the statutes of the database⁷. Examples of persons submitting data are other databases from which the data is obtained. This is seen as a tedious obligation. In practice, however, it would save the agency a significant amount of resources. Article 14 of the GDPR requires that if data is not received from the data subject, the data subject must be informed of the receipt of the data within a reasonable time. Clearly, this norm has not been implemented in practice. However, the person does not have to be informed if the receipt of the data is clearly provided for by law.

It is common for one agency to need data from another agency that it has collected for a different purpose. When connecting to and receiving data directly from the database of another agency, the data subject should be informed each time. The obligations of Articles 13 and 14 of the GDPR cannot be disregarded forever - the obligation to provide information must be introduced by all agencies in their work processes.'

7 View the dataset in the annex to the 'Statutes of social services and benefits', which is 11 pages long. https://www.migiteataja.ee/aktulisa/120/3201/9055/30M_05032019_m10li-sa2.pdf#

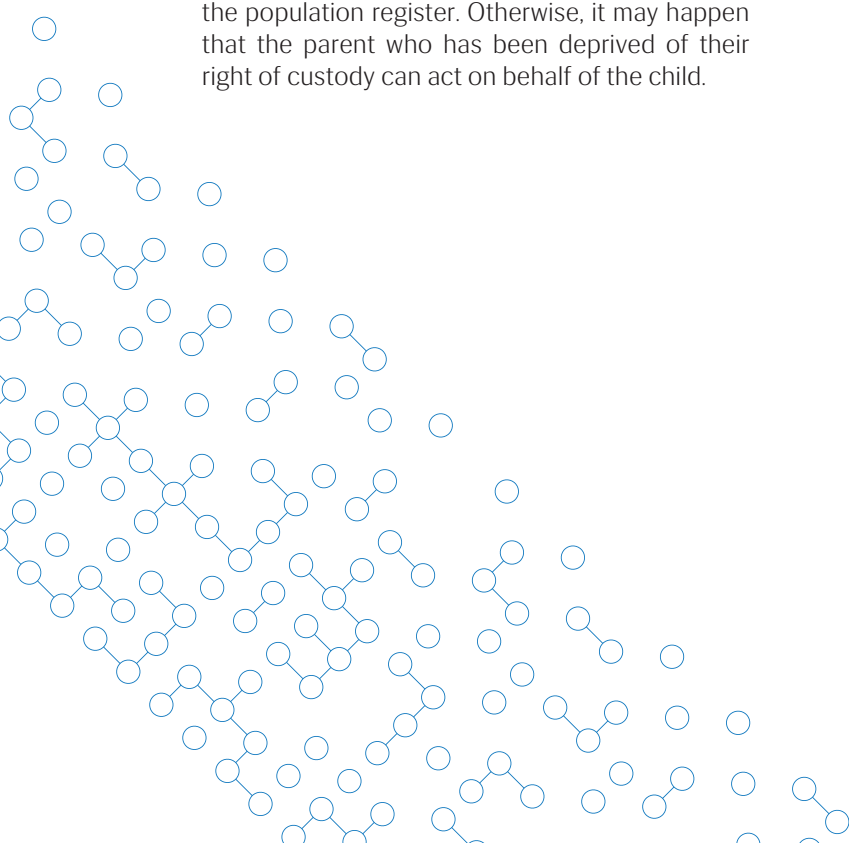
However, if the data exchange is clearly stated in law or in the statutes of the database, the obligation to notify the data subject each time could be avoided.'

Another issue that has come to the forefront last year is the misuse of inquiries from the population register. The following are the 3 most common errors.

- Firstly, the inquiry is too broad. It is only necessary to check the data of the person performing the operation in the information system, but an inquiry involving related parties is used for it. This causes the connected persons to ask why an agency with which they have nothing to do has viewed their data. In this way, the agencies do themselves a disservice.
- Secondly, an inquiry is made from the population register immediately upon entering the information system, although it is not required for entry. In other words, the inquiry is made prematurely.
- The third problem is the opposite of the first one – the inquiry is too narrow. In order to check the right of representation of a child, in addition to verifying their parent, it is necessary to check the existence and content of the right of custody in the population register. Otherwise, it may happen that the parent who has been deprived of their right of custody can act on behalf of the child.

For users of the standard solutions in the sense of the administration system for the state information system, it can be seen that they do not know how the system actually works, let alone it working in accordance with the instructions of the user as the controller. This means that when using the information system, the person who maintains the database cannot determine the retention periods or the scope of the data to be collected. It may also come as a surprise to them that sub-authorised processors from third countries are used in the processing.

'The focus of the Inspectorate in 2021 is data warehouses and open data'



JUDICIAL PRACTICE

While the legal director had a lot of work with drafts, less decisions were reached in judicial proceedings. The yearbook will address two of them. Unfortunately, both are decisions of courts of first instance. One was on personal data protection, the other on public information.

Case 3-20-375¹

Court decision in a personal data protection case

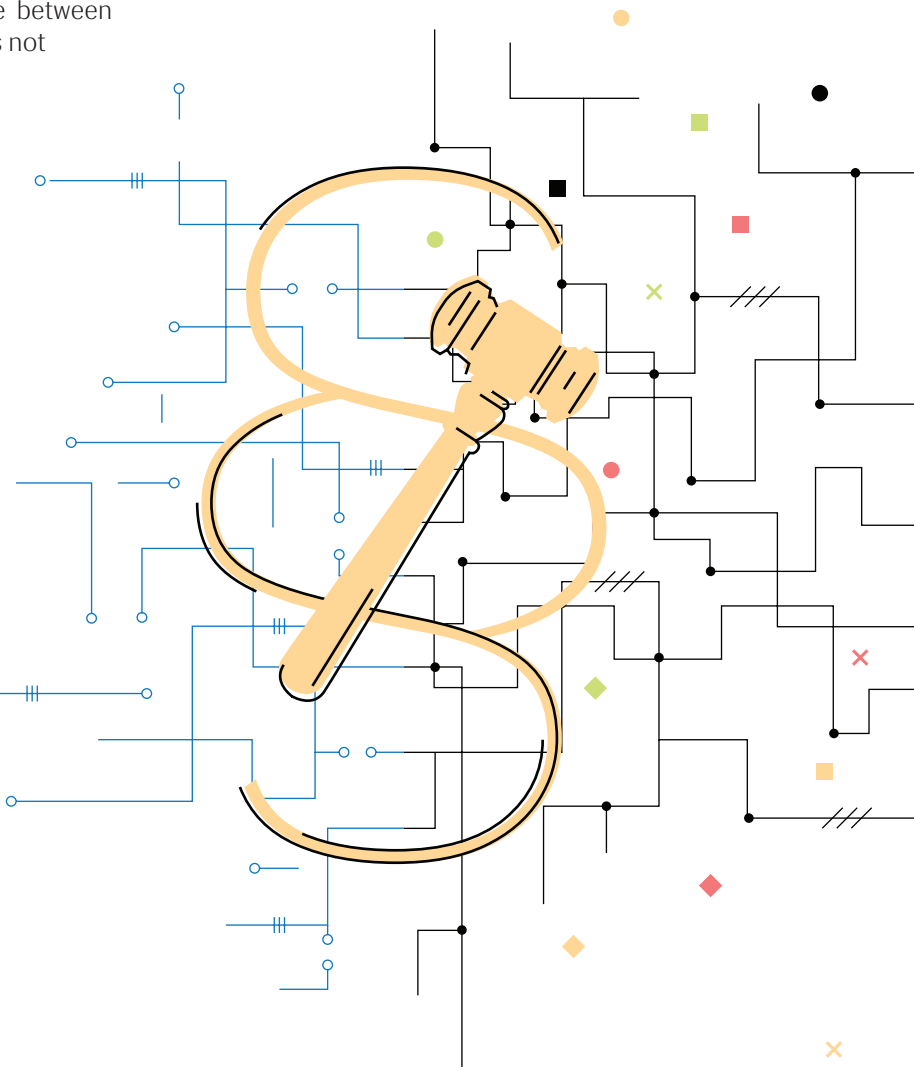
The Inspectorate was approached by two persons who had a dispute with the company where they had been a member of the management board. They contacted the Inspectorate because during the process of their removal from the management board, they were also deprived of access to their premises and information systems without prior notice, which left the company with their personal belongings and information, including files containing personal data. The company refused to issue them. First, the Inspectorate rejected their request to initiate proceedings as this was a dispute between two persons in which the Inspectorate does not

intervene – such disputes should be settled in a civil court. They challenged the failure to initiate proceedings in the challenge proceedings, but the challenge was also rejected and they then turned to an administrative court.

The reason why the Inspectorate maintained its position in the decision on the challenge procedure not to initiate proceedings was due to the fact that the Inspectorate is subject to the obligation to apply the Law Enforcement Act. Based on previous judicial practice, the Inspectorate can intervene in a dispute between persons in private law only if the conditions of subsection 4 (2) of the Law Enforcement Act are met.

¹ <https://www.riigiteataja.ee/captcha.html?r=%252Fkohtulahendid%252Ffail.html%253Fid%253D270987799>

Subsection 4 (2) of the Law Enforcement Act states that the adherence to the provisions of private law and the protection of the subjective rights and legal rights of a person are part of public order insofar as judicial legal protection is not possible in a timely manner, and without an interference by a law enforcement agency, exercising a right is impossible or significantly complicated, and to counter a threat is in the interests of public order. The Inspectorate had proceeded from the premise that we would intervene in a dispute between private individuals only if it was absolutely necessary or the person could not enforce their rights in court. The Inspectorate was also of the opinion that an application for action is not an application for the issuance of an administrative act, but an application for the initiation of proceedings, in respect of which the administrative authority has wide discretion. The data subject does not have the right to request the supervisory authority to implement a specific supervisory measure in the supervisory proceedings.



The court agreed that the Inspectorate had to proceed from subsection 4 (2) of the Law Enforcement Act. As the GDPR does not provide for a procedure for complaints submitted to supervisory agencies, national law must be followed in this respect. The corresponding provisions in Estonian law derive from the Administrative Procedure Act and the Law Enforcement Act. Thus, the Inspectorate had to follow, among other things, subsection 4 (2) of the Law Enforcement Act. However, the court said that in applying this provision, the Inspectorate had to interpret it in accordance with the GDPR to ensure its intended legal effect on the data subject. The court found that the Inspectorate had based its considerations only on the judicial practice before the entry into force of the GDPR and had not taken into account the rights arising from the GDPR for the appellants. As pursuant to Article 57 (4) of the GDPR, the supervisory authority may refuse to process a request where the request is manifestly unfounded or excessive, in particular because of its repetitive character, the court found that the request could be refused on the basis of subsection 4 (2) of the Law Enforcement Act if the request is clearly unfounded and excessive within the meaning of Article 57 (4) of the GDPR due to non-fulfilment of the preconditions of this provision.

The court further noted that it could be inferred from Articles 77 and 79 of the GDPR that the judicial protection of rights under the GDPR was without prejudice to the right of the data subject to lodge a complaint with the supervisory authority. Therefore, parallel proceedings are allowed. In other words, subsection 4 (2) of the Law Enforcement Act cannot be interpreted as meaning that if a person can apply to a civil court, the Inspectorate always has the right to refuse to process the complaint. The purpose of the GDPR is to ensure broad protection for the data subject and, pursuant to Article 57 (2) and (3), a person must be able to submit a complaint to the supervisory authority without difficulty and free of charge to protect their rights.

Therefore, a refusal to carry out a procedure should be exceptional. The court clearly states that in a situation where the complaint is not clearly unfounded or excessive, the Inspectorate has an obligation to process it.

The court ultimately concluded that the Inspectorate must reconsider the request and, if it still refuses to initiate proceedings, it must be justified why, despite judicial practice, the intervention threshold is not exceeded or provide explanations regarding the change of practice and how, as a result, it is a clearly unfounded or excessive complaint within the meaning of Article 57 (4) of the GDPR.

It was a decision that significantly changed practice. Namely, the Inspectorate is very often approached in disputes between private individuals. The most common are the so-called Facebook complaints, where one person has published some personal data about another with which the other does not agree. Following the court decision, we have the option of refusing to process such complaints. The Inspectorate naturally continues to recommend that individuals first defend their rights themselves. This means first asking the data publisher to remove them, but if this does not ensure the desired result, the inspectorate will be forced to intervene.

Given the limited human resources of the Inspectorate, such complaints play a significant role in the work load. At the same time, the complaint must be reviewed within 30 days pursuant to the Personal Data Protection Act. However, without underestimating the concerns of people and the need to protect their rights (for example, if data about them is published on Facebook without their consent), the Inspectorate mainly has to deal with resolving 'minor' complaints and interpersonal disputes, meaning that there are not enough resources to deal with major processors.

Case 3-19-2287²

Court decision in a public information case

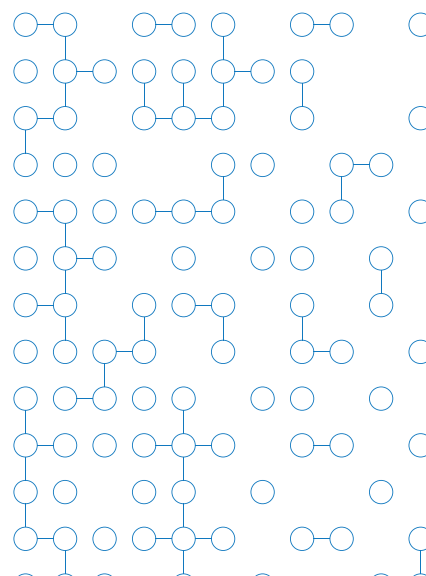
The persons had requested information from the City of Pärnu to obtain information on the expenses reflected in the appendix to its annual report. Namely, the annex contained data on all unusual transactions, one party to which is the City of Pärnu and the other party is a related party. The City of Pärnu refused to release such information on the basis of clause 23 (1) 1) of the Public Information Act, which states that the holder of information refuses to comply with a request for information if restrictions on access apply to the requested information and the person making the request for information does not have the right to access the requested information. The persons submitted challenges to the Inspectorate after the refusal, and the Inspectorate satisfied both challenges by obliging the City of Pärnu to reconsider the requests and issue the required information if there are no grounds to restrict access.

The position of the Inspectorate in both the decisions on challenge and court proceedings was that the holder of information is obliged to respond to the request for information. As the City of Pärnu took the view that the request for information could not be complied with, as the annex to the annual report for which information was requested is based on information requested from related parties and the related parties provided assessments of the transactions made by persons close to them with the City of Pärnu, which exceeded the scope of daily economic activities. The information also included answers to the question of whether they had made unusual transactions with the city. With an affirmative answer, the party to the transaction and the amount and balance of the transaction were specified, which meant that the information is subject to a restriction on access in accordance with the GDPR. The Inspectorate was of the opinion that the persons did not require the declarations to which the city refers, but contracts and other documents in a generalised form, the amounts of which are reflected in the respective annex to the annual report and which were the basis for compiling such an annex. The Inspectorate explained that the GDPR is not the general basis for setting a restriction on access; the basis for the restriction can be derived from the Public Information Act. On the one hand, the City of Pärnu confirmed that there were no restrictions on access to the documents, but on the other hand, it continued to refuse to release the information.

The court agreed with the Inspectorate. Although the City of Pärnu has explained that it distributes documents on the basis of such assessment criteria as 'procurement contracts that have raised questions about compliance with the Public Procurement Act' or 'unusual document', it has stated in the annual report that such transactions had taken place to the extent reflected in Annex 23. Thus, the City of Pärnu itself has assessed some contracts and documents as unusual, on the basis of which the corresponding amounts are also reflected in the annual report, which is why it must also know and understand which documents the persons wanted. The Inspectorate has also drawn the attention of the City of Pärnu to the fact that the holder of information has a duty to assist the person making a request for information if the content of their request is not understood, and not the other way around. The court also found that the requests for information described the requested information in sufficient detail.

The court noted that a holder of information (a local government agency) may not classify as internal documents concerning the use of budgetary funds of the local government and remuneration and compensation paid from the budget (clause 36 (1) 9) of the Public Information Act), information concerning the proprietary obligations of the holder of information (clause 36 (1) 10) of the Public Information Act), or information on the property of the holder of information (clause 36 (1) 11) of the Public Information Act). Thus, the information requested by the parties was public information that has to be provided to them.

² <https://www.riigiteataja.ee/captcha.html?r=%252Fkohtulahendid%252Ffail.html%253Fid%253D266920440>



The court also agreed with the Inspectorate that pursuant to subsection 3 (2) of the Public Information Act, access to public information can be restricted only pursuant to the procedure provided by law and the mere reference to the GDPR for the protection of personal data is not sufficient to set a restriction on access – the restrictions must be set on the basis of a specific provision of the Public Information Act. However, this does not mean that personal data should be disclosed if the restriction on access has not been erroneously imposed, and the Inspectorate did not claim this to be the case. As a result of the substantive and thorough proceedings, the court has rightly concluded that the non-compliance with the request for information was, in essence, unjustified. Although clause 35 (1) 12) of the Public Information Act obliges to classify as internal information which contains personal data if enabling access to such information significantly breaches the inviolability of the private life of the data subject, subsection 3 (2) and subsection 4 (3) of the Public Information Act impose an obligation to ensure the inviolability of the private life of a person when providing access to information without a separately established restriction on access. The holder of information has the right and obligation to assess in each individual case whether the right of the person making a request for information to have access to public information (subsection 44 (2) of the Constitution) or the right to the inviolability of private life of the data subject (subsection 26 of the Constitution) should be considered more important. If the interest in obtaining access to the requested information outweighs the interest of the data subject in the inviolability of their private life, the consent of the data subject is not required for the release of the information, as access to the information is provided by law.

The court further noted that although the city said it sought to protect the rights of the involved people by refusing to comply with the request for information, it did not understand how their rights would have been violated. The concluded contracts and other documents show how much and under what conditions different legal or natural persons have received public funds. It cannot be information which, by its very nature, requires protection. According to the City of Pärnu, these are mostly funds allocated to different legal entities.

Legal entities do not have private life or personal data to protect. This means that the disclosure of the names of members of the management bodies of such legal persons is permitted. The relevant information is also available from the commercial register. Receiving public funds is not a 'private economic activity', as the city has pointed out. Persons who receive local government budget funds must take into account the accompanying reporting and public scrutiny. Pursuant to section 1 of the Public Information Act, the purpose of the Act is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties.

Although this did not change the practice of the Inspectorate or provide legal clarity, the support of the court for the interpretations of the Inspectorate is important in such situations. In matters of public information, the Inspectorate seems to be in the role of an arbitration court, as the disputants are persons and information holders whose mediator the Inspectorate is.

Thus, the Inspectorate has a key role to play in shaping the practice of public information matters, as well as in interpreting legislation.'

This case also highlighted the desire of both the state and local governments to vigorously protect information in matters related to their use of money. A similar trend can often be seen with salaries, bonuses, and additional remuneration, but at the same time, situations where personal data needs to be protected are often not recognised.



THE DATA PROTECTION INSPECTORATE AND CROSS-BORDER CO-OPERATION

The Inspectorate is an active member of the European Data Protection Board and participates in several international working groups. Last year, it cooperated with the European Data Protection Board the most.

Since the entry into force of the GDPR on 25 May 2018, cross-border co-operation between data protection authorities has been completely reorganised compared to the time when the main form of co-operation was participation in the Article 29 Working Party. In short, the GDPR led to the implementation of a one-stop-shop system and a continuity mechanism. The first means that, regardless of the place of residence of the person (data subject) in the European Union, they may lodge a complaint with a data processor in another EU country and that the data protection authority will process the case or refer it to another national data protection authority. Such procedures are resolved and exchanged in the Internal Market Information System (IMI). The number of procedures exchanged through IMI in 2020 was 884.

Why is it necessary to deal with cross-border cases in this way and what does the continuity mechanism mean?

The reason lies in the nature of the GDPR itself. In other words, in the modern world of trade and technology, there are no longer 'classical' national borders. For example, we can buy goods from an e-shop in the Netherlands or consume the services of a company in Italy. It is therefore crucial that uniform data protection rules and the level of individual rights are guaranteed in all these countries. This can be ensured through the co-operation of data protection authorities, common procedures, common guidelines, etc. Decisions on the continuity mechanism are available on the website of the European Data Protection Board. Central to these decisions is the European Data Protection Board, which includes all data protection authorities of the member states, data protection authorities of the European Economic Area, and the European Data Protection Supervisor. The European Commission also participates in its work (albeit without the right to vote). Thus, the most important foreign co-operation of the Data Protection Inspectorate is participation in the work of the European Data Protection Board.

Due to the variety and volume of topics, the Data Protection Board has become a multi-level organisation. It would not be possible for a monthly general plenary (with the participation of the Directors-General of the agencies) to be able to draw up and analyse all the guidelines, positions, approvals, and other necessary decisions. Therefore, the European Data Protection Board also consists of sub-groups and task forces. There are 15 of them in total. The sub-groups and task forces are sector-specific, such as technology, social media, e-government, co-operation, etc. The Data Protection Inspectorate is one of the smallest data protection agencies in Europe (as we are one of the smallest agencies in Estonia), so we are forced to decide which are the priority topics for us in our development in international co-operation. Therefore, we are more active in some working groups of the Data Protection Board and passive in others.

The most widely heard views and guidelines which were drafted and approved by the Data Protection Board in 2020 concerned the transfer of data abroad.

It could be said that 2020 was the year of data transfers. In the summer, the long-awaited Schrems II judgment of the European Court of Justice was adopted, which affected the exchange of data with the United States, but Brexit and its impact on the exchange of data with the United Kingdom were also important. Following the Schrems II judgment, two very important guides for data processors were drawn up: recommendations on measures that supplement transfer tools and essential guarantees on surveillance measures.

However, 2020 was also the year of the coronavirus pandemic and required a number of explanations and instructions on how data processing should work in the new situations. For example, guidelines were developed on the admissibility of processing location data and the use of health data for coronavirus research, and a position was issued on data processing in the context of the coronavirus.

Previously issued guidelines on consent and the roles of controller and processor were also updated. The nature of the articles of the GDPR was also clarified, such as the application of Article 23.

Guidelines were also produced on more specific topics, such as a guideline on connected vehicles in the technical field, a guideline on the second payment services directive and a guideline on the GDPR in the financial sector, and a guideline on targeting users in the field of social media.

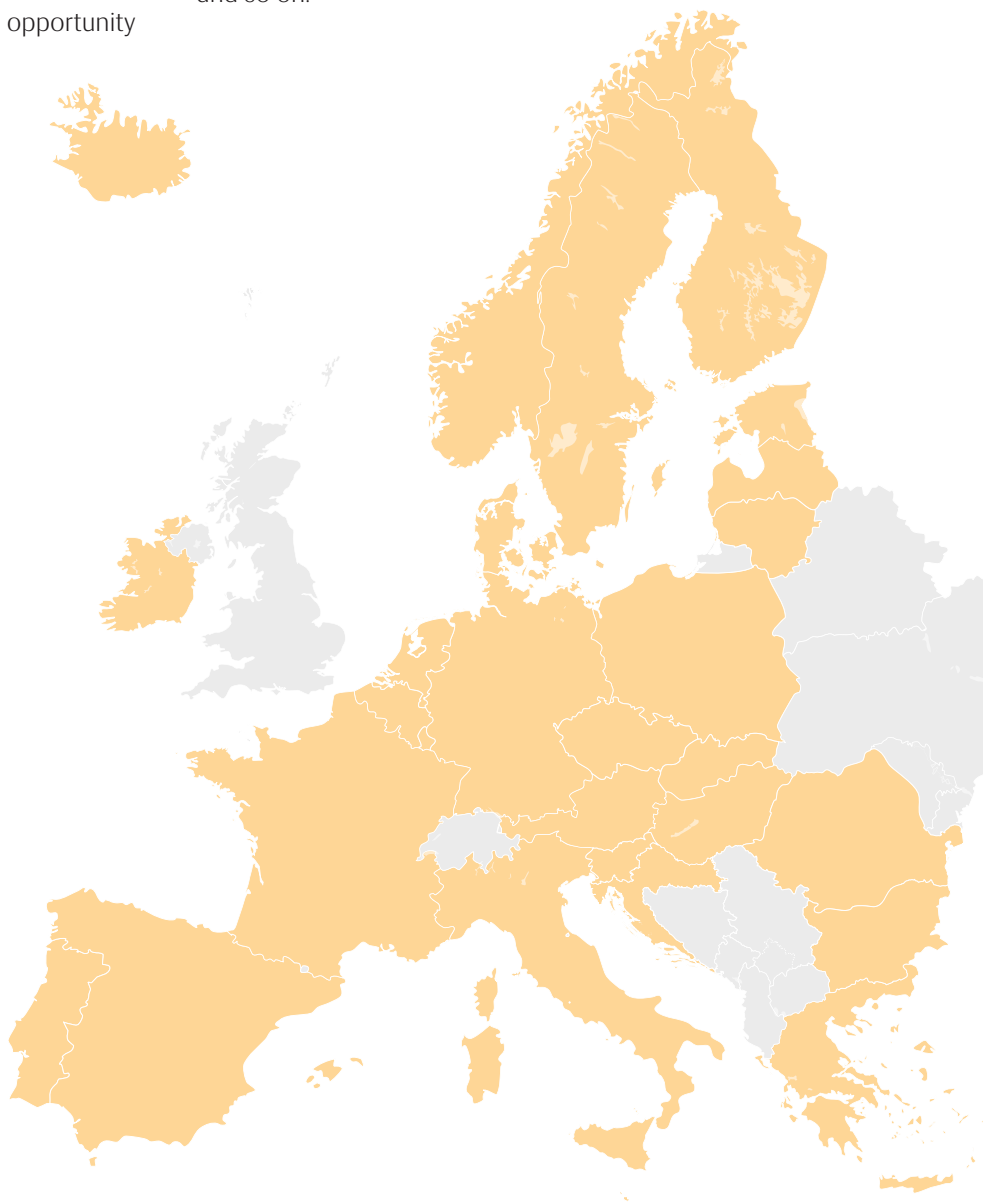
The usual practice of the European Data Protection Board in drafting guidelines is to refer them to a public consultation, giving everyone the opportunity to express their views on the guideline or recommendation. Several of the guidelines mentioned above have just completed their public consultation procedure and have not yet been finally approved.

Convention 108

The European Data Protection Board was not the only foreign co-operation partner of the Inspectorate, but given the special nature of 2020, there were no major international conferences which are usually considered one of the highlights of the year. Nonetheless, online meetings of the data protection committee of Convention 108 still took place. The Inspectorate was able to provide input on a number of guidelines and approved a number of indicative guidelines, such as on facial recognition, child data processing and education, profiling, digital identity, and so on.

Members of the European Data Protection Board are

Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Norway, Iceland, and Liechtenstein. The European Data Protection Supervisor is also a member of the European Data Protection Board.






ACTIVITIES IN NUMBERS

The number of violation reports increased

In 2020, the Data Protection Inspectorate received 138 violation reports, which was 20% more than a year earlier. The most common reason for the reports was negligence, carelessness, and mistakes caused by ignorance. Other reasons included violations caused by software errors and planned malicious actions with customer databases, as well as phishing scams and ransomware attacks.

A quarter of all violations reported to the Inspectorate were related to the consequences of phishing scams or ransomware attacks. The private sector reported the highest number of phishing scams. Both public and private data processors reported ransomware attacks. Of the 138 violations, 54 or 39% concerned the public sector.

The Inspectorate received about 20 violation reports due to a software error or malfunction. For example, there was a violation where people received an email regarding the decision of a service provider that was actually intended for someone else. This was due to an error in entering information into the automated decision system and the decision was therefore sent to hundreds of wrong email addresses. The relevant parties discovered the error themselves and the violation was brought to an end quickly without the intervention of the inspectorate.



Software-related incidents sometimes take place due to the simultaneous occurrence of completely unforeseen circumstances. For example, a trading company had a case where two different people simultaneously signed the loyalty programme agreements in the e-service of the company. The information system interpreted this as a single operation and stored only the contract of one person, but the customer profile of both people. As a result, the data of one person became available to the other. Technical problems occurred in both the public and private sectors. The Inspectorate also registered cases caused by a weak or outdated security solution. For example, by knowing the password of a colleague, it was possible to access the information system without leaving a trace of the actual viewer of the data. In one case, a criminal accessed the information system of an educational institution because a VPN connection was not established.

The most common cases were ones which could have been avoided if the employee had been more attentive and careful.'

Such incidents accounted for more than half of all violation reports. Many human errors occurred in the public sector, such as a document containing sensitive content in relation to online services and document registers being made public or accessible to people who should not have had access to this information.

There were cases where information about the wrong person was issued by telephone in both the private and public sectors. This happened because the identity of the caller was not sufficiently verified.

In 2020, more thefts of customer databases were reported than in previous years. All the cases were connected by the fact that the customer databases were copied from the information system and taken to the new job. The employees either started working for another employer or started providing a similar service themselves.

Incidents were most common in the health, social, and financial sectors. This generalisation does not provide information on the most problematic data processors. Instead, it shows responsible behaviour and greater awareness. It is the responsibility of each data processor to register a data breach and, in certain cases, to notify the Inspectorate if there is a likely risk to human rights and freedoms. The information must be provided to the Inspectorate within 72 hours of the incident. In the event of a serious risk, the data processor must also inform the persons concerned.

The Inspectorate initiated supervision proceedings against registered violation reports in approximately one third of the cases to establish the circumstances and prevent similar incidents in the future.'

THERE WERE FEWER CALLS TO THE HOTLINE THAN LAST YEAR

In 2020, the hotline of the Inspectorate was called a total of 1,222 times. A year ago, the total number of calls was 1,578. The lower number of calls may have been due to the fact that the coronavirus affected the reorganisation of work and therefore, the hotline was not open all the time in March and the working time of the hotline was also shortened.

The main reason for calling the hotline was the use of security cameras. Approximately 250 calls were made to ask about obligations of the security camera owner, the violation of human rights, and the punishment of the offender. The use or misuse of security cameras was also discussed in other calls where the main reason for the call was another data protection issue. Video surveillance organisers mostly called to ask why video surveillance has rules.

Other calls concerned data disclosure and dozens of other issues related to the implementation of data protection.

The main concerns were the publication of data on the Internet, in media publications, social media, and on websites. People also had concerns about closing their email address after leaving work.

As a new topic, people asked how to request data about themselves.'

Advice was also sought on the implementation of the GDPR in accordance with their operational specifications. Clarifications were also requested on how to ask for consent and what the data protection conditions should be. Callers were also interested in what should be included in the contracts between the controller and the processor and how to carry out an impact assessment or how to appoint a data protection officer.

Calls related to apartment associations concerned the use of cameras on the territory of the association. The most frequently asked questions about debt were about the disclosure of debt data by debt collectors and enforcement agents, e.g. whether a debt collector can inform the employer about the debt.



THE NUMBER OF DATA PROTECTION SPECIALISTS IS GROWING

The contact details of the appointed data protection officers have been published on the Company Registration Portal since 25 May 2018. By the end of the same year, 2,782 data protection specialists had been appointed. In 2019, 1,016 specialists were appointed, and in 2020, 375.

As at 31 December 2020, 4,173 data protection specialists had been listed on the Company Registration Portal of the Estonian commercial register.

Legal order	2018	2019	2020
A legal person governed by public law, a constitutional institution, or an agency thereof	18	22	26
Local government agency	328	668	666
Authority of executive power or other national institution	99	121	118
Register of state agencies	445	811	810
Non-profit association	238	341	404
Foundation	90	107	114
Commercial association	3	7	7
Non-profit associations and foundations register	331	455	525
Public limited company	221	240	231
European company (Societas Europea)	4	4	4
Self-employed person	42	50	49
Private limited company	1,664	2,127	2,419
Commercial association	24	28	28
General partnership	4	5	6
Limited partnership	6	8	9
Branch of a foreign company	21	25	24
Commercial register	1,986	2,487	2,770
Apartment association			
Register of apartment associations	20	45	68
Total	2,782	3,798	4,173

STATISTICS OF THE YEAR

ACTIVITIES	2017	2018	2019	2020
Guidelines (excluding updates)	2	1	-	1
Opinions on draft legislation	34	42	8	29
Awareness-raising				
Requests for explanation, memorandums, statements of claim, and requests for information	1,520	2,384	2,343	1,759
Calls to the hotline	1,527	2,556	1,578	1,222
Consulting (for companies, institutions)	148	200	79	60
Consulting (for companies, institutions)	17	23	15	11
Supervisory work				
Circulars (without initiating supervision)	4	8	2	2
<i>Including recipients of circulars</i>	26	162	110	1,108
Large-scale comparative monitoring	10	2	-	1
<i>Including the number of persons monitored</i>	129	85	-	77
Complaints, challenges, reports of misdemeanours (submitted) on the basis of the Personal Data Protection Act, the Public Information Act, and the Electronic Communications Act	462	462	609	701
Requests through IMI (EU information system through which data protection authorities exchange information and other requests)	-	479	1,048	884
Self-initiated supervision (initiated)	149	15	29	28
<i>Including preventive data protection audits</i>	1	1	0	0
On-site visits (supervision)	45	17	0	2
Recommendations and suggestions (supervision)	125	10	63	223
Precepts (usually preceded by a suggestion; usually includes a penalty payment warning)	64	46	14	37
<i>Including registration (without prior suggestion)</i>	35	-	-	-
Misdemeanour cases (closed)	9	23	14	12
Fines (misdemeanour penalty), penalty payment (supervision)	4	9	5	12
Authorisation and special procedures				
Requests for approval of databases (for establishment, introduction, change of data set, termination)	99	36	39	16
Applications for authorisation of research without the consent of the data subjects	54	61	30	32
Applications for permission to transfer personal data abroad	22	3	1	2
Requests for own data in Schengen, Europol, and other cross-border databases	8	21	31	10
Number of employees and budget of the Inspectorate				
Permanent posts	19	19	19	19
Annual budget (thousand euros)	714	717	750	751

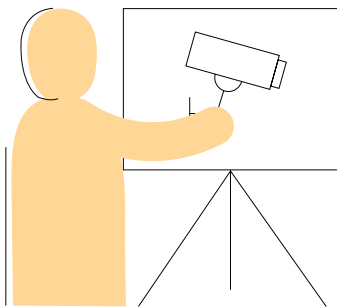
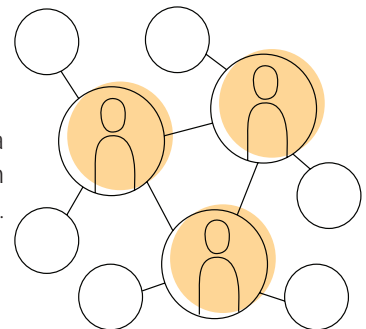
LOOKING AHEAD

Last year, the Inspectorate conducted an anonymous survey of selected partners to obtain feedback on the work done so far. The Inspectorate also asked them what it should be like in 2024. The following is a vision of their expectations for the Inspectorate. We will have to wait and see whether they were right.



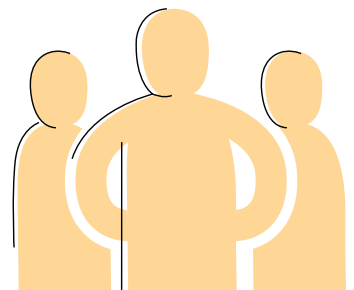
The Data Protection Inspectorate is an institution that prevents, guides, advises, and drives discussion in society. The Data Protection Inspectorate is fast, efficient, and, if necessary, forceful.

The Data Protection Inspectorate is a partner and has cooperation networks (with data protection specialists, for example).



The Data Protection Inspectorate offers newsletters, trainings, and guidelines. Communication through digital solutions is easy, fast, and convenient.

The Data Protection Inspectorate is funded and staffed.



The name of the Data Protection Inspectorate is outdated and refers only to supervision and punishment, not to partnership and counselling.

A request for information came
the email was pretty mad,
issue the protocol,
that is what they pay you for.

More requests kept flooding in,
issue this, issue that,
asking for memos, directives,
had to find them to keep the peace.

Does it not make you mad?
Some people do this day after day.
I sip my coffee and think to myself,
'Does anyone know how to act?'

The discussion got heated,
the growing workload caused tensions,
the boss also came for a coffee
and gave plenty of 'help'.
They said, 'Get right back to work!'
Read through the Public Information Act,
it is not that long at all.

So I went back to my desk
and saw an invitation to AKI's Information
Day
My first question was,
'What should I do now!?'
...

Finally, they got around
to sending the documents.
I asked for an extra 100 pages,
'Could you make me copies of them?'

I needed those files very much –
I had to know how a village building was built.
I did not want to annoy them,
I just needed the information.

When a friend heard about the request,
they said not to make a big deal of it.
Who needs all these papers?
But what does he know?

His construction company is going bankrupt.
I know what is right
and I am on the right path.

- S. Heiberg

On the occasion of the International Day for
Universal Access to Information, a conference was
held on 29 September where the employees of the
Inspectorate discussed topical issues in the field of
public information. The conference began with
Contra reading the first poem on public information
law in Estonia.

