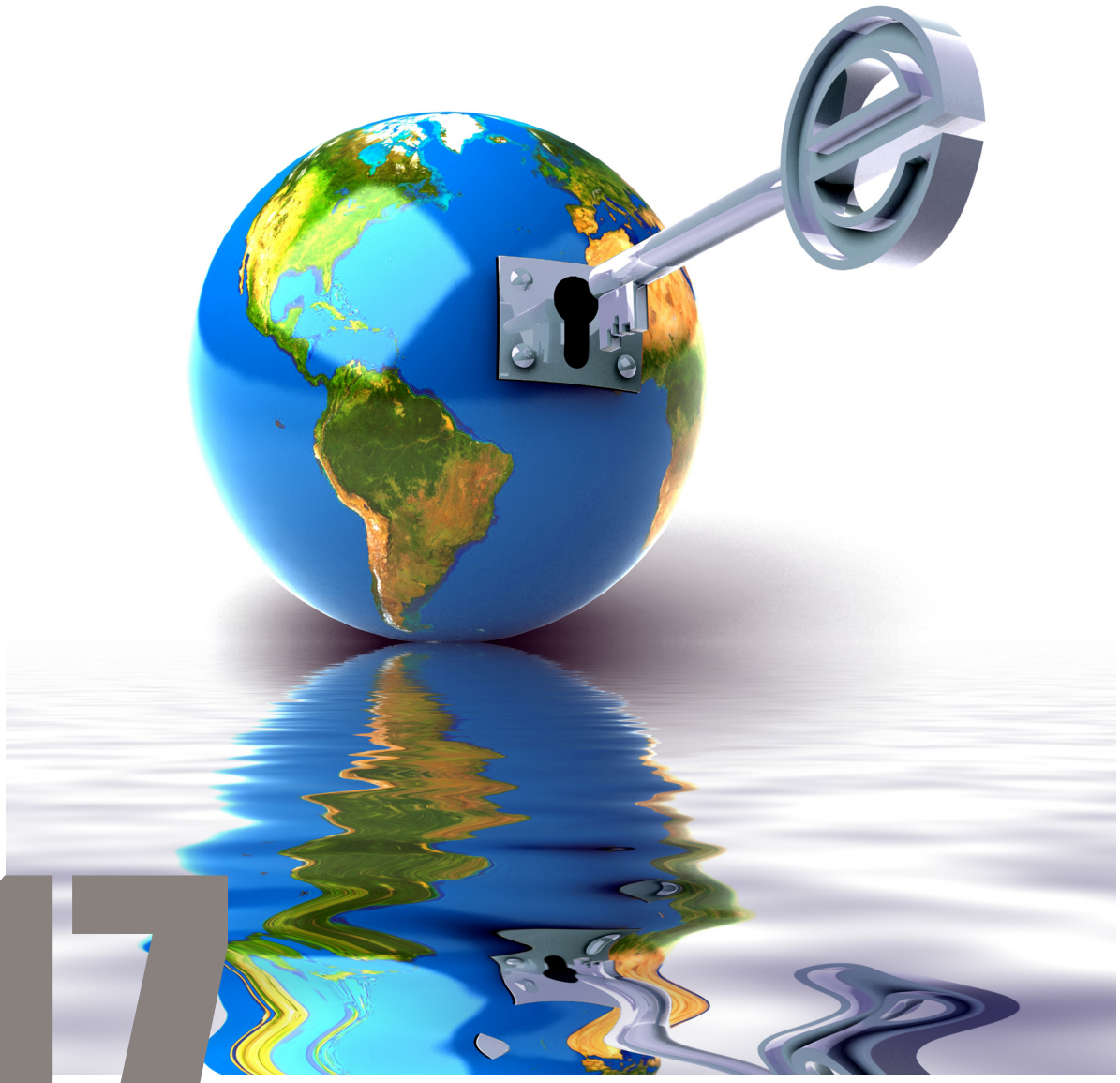
Information Commissioner of the Republic of Slovenia



'17 Annual report

Introduction by the Information Commissioner

One of the key activities of the Information Commissioner in 2017 were the preparations on the entry into force of the new European General Data Protection Regulation. This also guided the Information Commissioner's cooperation with individuals, enterprises and other organisations, for whom the Information Commissioner issued numerous opinions and conducted many trainings and meetings. The upcoming entry into force of the GDPR particularly characterised the international activities of the Commissioner, namely in the framework of the group of data protection supervisory authorities, the Working Party 29. The opinions of the Information Commissioner on draft legislation were also influenced by the new EU Regulation, including the proposal for a draft law on personal data protection. Above all, the desire to protect the rights of individuals to the greatest possible extent led the Information Commissioner to try its best to swiftly resolve the complaints in the field of access to public information and to take effective action against violations of personal data protection. In both legal fields, the Information Commissioner also conducted many trainings.

In the area of access to public information, it is welcoming to note that there has been a reduction in the number of complaints against the actions of municipalities, which arguably demonstrates a better management of municipalities in this area in 2017, especially in comparison to previous years when showed a much lower response rate of municipalities in access to information procedures. However, the applicants filed more complaints against state authorities this year, and the number of requests for clarifications and opinions from bodies liable increased again. All of the above shows that bodies liable were more active and responsive in 2017 than the year before, also due to the fact that they contacted the Information Commissioner even outside the complaints procedures.

In 2017, the Information Commissioner received 522 complaints in the area of access to public information, which is more than the previous year when it received 514 complaints. The Commissioner endeavoured to resolve the complaints swiftly and without undue delay for the applicants. The average time for resolving the complaints against refusal decisions with special examination procedure required was 37 days. The complaints were thus resolved much more quickly than within the statutory two-month time-limit for resolving such matters laid down in the General Administrative Procedure Act. By comparison, in 2016, the average time of resolving the complaints was 47 days.

The Information Commissioner dealt with several important cases as to their substance matters in the complaints procedure. With regard to the exceptions invoked by the bodies liable, it should be noted that there was an increase in the number of cases concerning the so-called "abuse of justice" exception. However, this institute should be used as a last resort that may only be invoked by the bodies liable in exceptional cases. This is because the right to access to public information as a fundamental human right should only be restricted for the protection of legitimate interests and rights of others and the restriction should be kept at such minimal level that the protection of such interests of others is still guaranteed.

The data indicates that in 2017, the structure of the applicants who appealed to the Information Commissioner partly changed. In this year too, the highest number of complaints were filed by natural persons, the number of complaints by private legal entities decreased, while the number of complaints filed by journalists remained for the most part the same. It is interesting to note that the number of complaints involving legal entities of the public sector increased, indicating that the right to access to public information is an institute that allows various categories of applicants to obtain information quickly and efficiently. In view of the increasing number of complaints, it can be concluded that applicants are well aware of the access to information procedure and that this procedure is fast, efficient and cost-free, which means that it provides an effective legal protection.

In 2017, the Information Commissioner handled 655 inspection cases, including 226 in the public and 429 in the private sector, and it conducted 105 minor offence procedures. It also received 16 requests to connect personal data filing systems, four requests to allow the implementation of biometric measures, 29 requests for transfer of personal data, and 110 complaints against decisions to refuse access to personal data.

The majority of reports on suspected violations of personal data protection legislation were made due to the transmission of personal data to unauthorized users, unlawful collection or transmission of personal data, the use of personal data for direct marketing purposes (in particular, for suspected unlawful obtaining of personal data for these purposes and the failure to comply with the individual's request to no longer use personal data for these purposes), the implementation of video surveillance and unlawful use of the

recordings (especially in workplaces), inadequate security of personal data, the use of personal data contrary to the purpose of their collection and unlawful access to personal data. It should be noted that the number of reports and violations found with regard to inadequate security of personal data collected or made available through online networks increased. The reason for the increase lies in large part with numerous hospitals and other health care institutions that offer electronic appointment system that did not provide secure connections for the operation of this system (e.g. by using the https protocol or appropriate encryption). For this reason, after conducting a systematic supervision, the Information Commissioner urged all health care institutions to remedy these deficiencies. The Information Commissioner repeatedly found in inspections the failure of other liable entities of securing personal data on web servers with personal files with restricting access with a firewall, username and password, or otherwise.

The Information Commissioner also recalls that there has been an increase in the number of reports due to the unlawful collection or transmission of personal data as a result of insufficient or inadequate information provided to data subjects. The new European General Data Protection Regulation, which will come into force on 25 May 2018, is even stricter with regard to transparency requirements than the valid ZVOP-1. Namely, Article 13 (2) and (3) enlist a wide range of information which shall be provided to the data subject.

In addition to handling the reports it received, the Information Commissioner continued in 2017 with the enhanced performance of the so-called planned ex officio inspections in areas where, according to the risk assessment, there was a greater likelihood of violations of personal data protection legislation. The planned supervision of compliance with the provisions of the ZVOP-1 was performed in ministries, administrative units, health institutions, major data processors, tourist agencies, trade unions and their federations and associations and their federations.

In addition to inspection and minor offence procedures, the Information Commissioner in 2017, with the aim of preventing violations, paid special attention to providing support to companies. It also responded to 1.289 requests for written opinions and clarifications in the field of personal data protection and 1998 telephone calls. The Information Commissioner was also contacted by more than 115 controllers and processors from the public and private sector during drafting of laws and regulations, preparing solutions or projects, who wanted to reflect on the risks of such new processes in a timely manner to avoid breaches of the law. With the aim of ensuring compliance with the new Regulation in time and as part of its preventive action, the Information Commissioner also held 132 lectures for various companies and other organizations. Same as every year, the Information Commissioner experts participated in various conferences, lectures, professional events, consultations and round tables to raise awareness of the importance of privacy and personal data protection.

It was clear in 2017 that large controllers have already started with intense preparations to the upcoming GDPR, while some of the smaller controllers who up until now were excluded from complying with several provisions of the ZVOP-1 (e.g. establishing filing system catalogues reporting personal data filing systems to the Information Commissioner) were less acquainted with personal data protection legislation. For some data controllers and processors designating the data protection officers also represents a specific challenge. The institute of the data protection officer has been thus far known especially in banks and insurance companies, while the GDPR now provides for quite a wide range of liable entities who shall designate such an officer. Namely, the designation is obligatory when processing is carried out by a public authority or body, except for courts acting in their judicial capacity; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Within the scope of its international cooperation, the Information Commissioner organized in May 2017 the first constituent session of the “Initiative 20i7” in Bled, Slovenia, hosting the heads of data protection supervisory authorities from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo and Macedonia. The Information Commissioner’s initiative follows the example of the Nordic countries, which share similar historical and legal backgrounds and their personal data protection supervisory authorities cooperate closely and share experiences. It is precisely in the light of the personal data protection reform at the EU level that the Initiative has proven to be a particularly effective way of sharing good practice and experiences useful in the preparations for the entry into force of the GDPR.

There are many challenges ahead in 2018, particularly those related to the entry into force of the new European General Data Protection Regulation. At the same time, it is already possible to see that the new European legislation brought a breath of fresh air to the field of privacy protection in Europe and in the world. It seems as if personal data protection is being reinvented. The Information Commissioner will strive to make the most out of this new regulatory wind in Slovenia. As a member of the new European body, the European Data Protection Board, the Information Commissioner will be actively involved in the preparation of the European guidelines and other preventive mechanisms that the Board will prepare, and as a supervisory authority will participate in national and international inspections under the auspices of the Board. Since the Republic of Slovenia has not adopted a new law on personal data protection by 25 May 2018, the companies, other organizations and the Information Commissioner face many challenges and are tasked with many additional responsibilities. The work the Information Commissioner will have to do will be demanding, and the absence of an organic law makes things all the more difficult. Nevertheless, I am convinced that the Information Commissioner will continue to effectively protect both constitutional rights in the future. Our main concern is preventive action, efficient complaint handling and responsible conduct of inspections.

Mojca Prelesnik,
The Information Commissioner

1 THE INFORMATION COMMISSIONER

1.1 THE ESTABLISHMENT OF THE INFORMATION COMMISSIONER

On 30 November 2005 the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act (Official Gazette RS, Nos. 113/05 and 51/07 – ZUstS-A, hereinafter: the ZInfP), establishing a new and independent state authority as of 31 December 2005. The Act combined two authorities, namely the Commissioner for Access to Public Information and the Inspectorate for Personal Data Protection. Upon the entry into force of ZInfP, the Commissioner for Access to Public Information continued the work as the Information Commissioner and took over the inspectors and other staff of the Inspectorate for the Protection of Personal Data, the equipment and assets. At the same time, it took over all pending cases, archives and records kept by the Inspectorate for the Protection of Personal Data. Thus, the responsibilities of the body responsible for the implementation of the right to access to public information changed significantly and expanded to the field of personal data protection. The Information Commissioner thus also became the national supervisory authority for data protection. It commenced its work on 1 January 2006.

Mojca Prelesnik is the head of the Information Commissioner as of 17 July 2014.

1.2 KEY AREAS OF PERFORMANCE AND MAIN COMPETENCES OF THE INFORMATION COMMISSIONER

The Information Commissioner performs its statutory tasks and competences in two fields:
- In the field of access to public information;
- In the field of the data protection.

In accordance with Article 2 of the ZInfP, the Information Commissioner is competent to:
- decide on appeals against a decision by which an authority denied or refused the applicant's request for access or in any other manner violated the right to access or re-use public information, and also, within the frame of complaints procedure, to supervise the implementation of the act regulating access to public information and regulations adopted thereunder (as the appellate authority in the area of access to public information);
- perform inspections regarding the implementation of the Act and other regulations governing the protection or processing of personal data or the transfer of personal data out of the Republic of Slovenia, as well as to perform other duties determined by these regulations;
- decide on the appeal of an individual against the refusal of a data controller to grant the request of the individual with regard to his right to access requested data, and to extracts, lists, viewings, certificates, information, explanations, transcripts, or copies in accordance with the provisions of the act governing personal data protection;
- file a request before the Constitutional Court of the Republic of Slovenia for the review of the constitutionality of a law, regulation, or general act issued for the exercise of public authority if a question of constitutionality or legality arises in connection with proceedings it is conducting, in both the field of access to public information and personal data protection.

In the area of access to public information, the Information Commissioner also has the competences determined by the Mass Media Act (Article 45, hereinafter: the ZMed). A liable authority's refusal of a request by a representative of the media shall be deemed a decision refusing the request. The authority competent to decide on appeals is the Information Commissioner.

The Information Commissioner is also responsible for managing the record of all exclusive rights granted in the field of re-use of information (Article 36a, Paragraph 5 of ZDIJZ).

The Information Commissioner is competent under the Patients' Rights Act (ZPacP), the Travel Documents Act (ZPLD-1), the Identity Card Act (ZOIzk), Electronic Communications Act (ZEKom-1), Central Credit Register Act (ZCKR), Consumer Credit Act (ZPotK-2), Decree on unmanned aircraft systems and Decree on the implementation of the Regulation (EU) on citizens' initiative.

With the entry of the Republic of Slovenia into the Schengen Area, the Information Commissioner also assumed responsibility for supervision of the implementation of Article 128 of the Convention Implementing the Schengen Agreement and is thus an independent body responsible for supervising the transfer of personal

data for the purposes of the mentioned Convention.

1.3 ORGANISATIONAL STRUCTURE OF THE INFORMATION COMMISSIONER

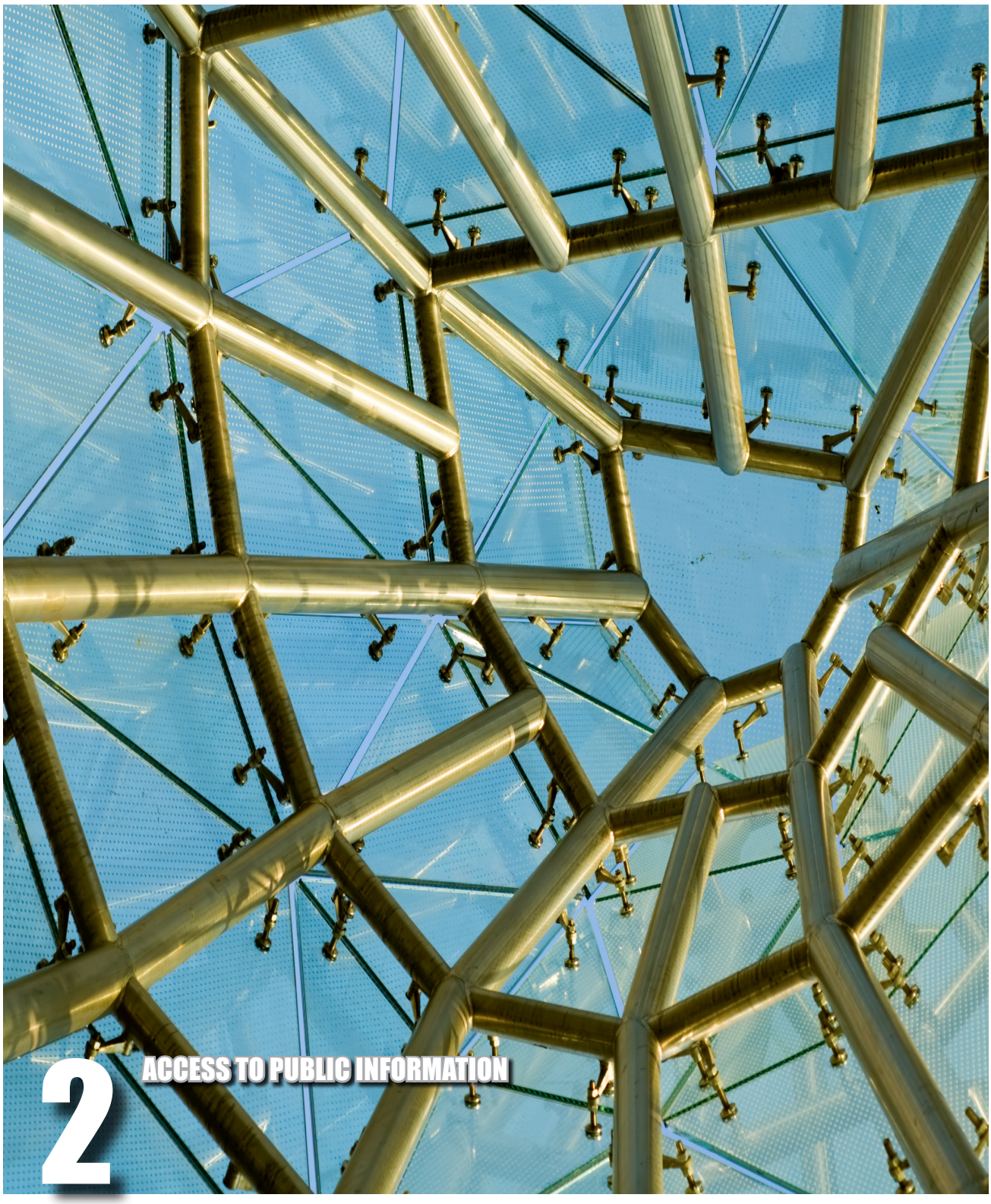
The Information Commissioner carries out its tasks through the following organisational units:
- The Secretariat of the Information Commissioner;
- The Public Information Sector;
- The Personal Data Protection Sector;
- Administrative and Technical Services.

At the end of 2017, the Information Commissioner had 34 employees, of which two were employed on the basis of temporary contracts.

1.4 FINANCIAL ASSETS OF THE INFORMATION COMMISSIONER

The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia on the proposal of the Information Commissioner (Article 5 of the ZInfP).

In the fiscal year 2017, the operating budget of the Information Commissioner amounted to EUR 1,459,747.90, of which EUR 1,306,000.00 were spent on wages and salaries, EUR 134,247.90 on material costs and expenses and EUR 19,500.00 on investments. Material costs and expenses were necessary for the normal functioning of the Information Commissioner (stationery, travel expenses, cleaning expenses, student work payments, postal services, the education of employees, producing brochures, etc.).



2 ACCESS TO PUBLIC INFORMATION

2.1 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

The right to access public information was granted by the legislature already in the Constitution of the Republic of Slovenia. The second paragraph of Article 39 of the Constitution determines that everyone has the right to obtain information of a public nature in which they have a well-founded legal interest under law, except in such cases as are provided by law. This right is further regulated in the Access to Public Information Act (hereinafter: the ZDIJZ). The bodies liable under the ZDIJZ are divided into two groups:

- Bodies, i.e. State bodies, local government bodies, public agencies, public funds and other entities of public law, public powers holders and public service contractors;
- Liable business entities subject to dominant influence of entities of public law.

The bodies liable are obliged to provide public information in two ways: by publishing it on the Internet and by providing access upon individual requests.

ZDIJZ provides the right to access information that has already been created and exists in any form. Thus, this act provides for the transparency of the use of public money and the decisions of the public administration, which should work on behalf of the people and for the people.

In 2017, the Information Commissioner received 522 appeals, of which 321 were against decisions refusing requests, while 201 were against the non-responsiveness of first-instance authorities.

In appeal procedures the Information Commissioner issued 316 decisions on the merits, in four cases it rejected the appeal, while two applicants withdrew their appeals. In processing the appeals of individuals, 61 so-called in camera examinations were carried out.

The Information Commissioner received 201 appeals against the non-responsiveness of the authorities. The Information Commissioner first called on to the liable authorities to decide on the requests as soon as possible, which in most cases they did. In 16 cases the Information Commissioner rejected the appeal (in 15 of those cases because the appeal was lodged too soon and in 1 case because the application was incomplete). The Information Commissioner explained to one applicant that his application was lodged too soon, in 2 cases it issued the explanation that it was not competent to consider their applications and advised the individuals how to act. 8 applicants withdrew their appeals as they received the requested documents and in one case the Information Commissioner transferred the matter to a competent authority for consideration. In one case, the Commissioner filed a report to the administrative inspection for the breach of provisions of the ZDIJZ and ZUP - the General Administrative Procedure Act.

In 2017, the Information Commissioner received 324 written requests for assistance and various questions of individuals regarding access to public information. During business hours the Commissioner also answered 729 telephone calls about questions from the field of access public information. The Information Commissioner replied to all applications to the extent it is competent, in most instances it referred them to the competent institution – The Ministry of Public Administration.

In 2017, 50 appeals were filed with the Administrative Court against decisions of the Information Commissioner (i.e. against 15,8 % of the decisions issued). The relatively small portion of such appeals indicates a greater level of transparency and openness in the public sector in relation to its operations and the acceptance of the Information Commissioner's decisions by various authorities and applicants.

The Administrative Court issued in 2017 31 judgments in relation to appeals filed against the decisions of the Information Commissioner. In 19 cases the Court dismissed the appeal, in 10 cases the Court granted the appeal and returned the matter to the Information Commissioner for reconsideration, in 1 case it partially rejected the appeal and partially granted it and returned the matter in relevant part to the Information Commissioner for reconsideration and in 1 case it issued a decision staying the proceedings.
The following actions were taken amongst the decisions issued by the Information Commissioner:

- in 144 cases it dismissed the appeal;
- in 123 cases it partially or fully granted the appeal of the applicant or decided in favour of the applicant;
- in 44 cases it granted the appeal and returned the matter to the first instance body for reconsideration;
- in 3 cases it rejected the appeal;
- in 2 cases it declared the first instance decision null.

The following categories of bodies liable were the subjects of Information Commissioner's decision in the appeal process as they refused access to public information:

- public administration (ministries, constituent bodies, public administration units) (155 cases);
- public funds, institutes, agencies, public service contractors, and holders of public authority (113 cases);
- municipalities (41);
- liable business entities subject to dominant influence of the state, municipalities and other public law entities (7).

In 211 cases applications were submitted by natural persons, in 65 cases complaints were submitted by private sector legal entities. 33 complaints were submitted by journalists and 7 by public sector legal entities.

In 2017, the Information Commissioner initiated one minor offence proceeding under Para. 2, Article 39 of the ZDIJZ, because the body liable permanently deleted the requested documents after receiving the request for access to public information, with the purpose of preventing the information from becoming public. The case has not yet been concluded.

2.2 SELECTED CASES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

The scope of work, business secret (decision number 090-153/2017)

The applicant requested from the Public Company Vodovod - Kanalizacija d.o.o. (water and sewage company) access to specific parts of the business cooperation agreements between the body and several multi-apartment building managers. The body denied access, claiming that the requested agreements were not related to its public-law responsibilities and contained business secrets. The Information Commissioner, however, concluded that the requested agreements fall within the body's scope of work and that certain data within the agreements cannot be classified as business secret. Namely, the Information Commissioner found that in this regard the body is a user of public funds in connection with the performance of the public service in question and that data on the use of public funds is public on the basis of the law (namely, the ZDIJZ) and therefore cannot be classified as business secret. Thus, the Information Commissioner decided that the body is obliged to provide the requested information to the applicant. With regard to the rest of the requested information, the Commissioner concluded that it does not relate to the use of public funds and can therefore be protected as a business secret. In this part, the Information Commissioner rejected the applicant's complaint.

Abuse of rights (decision number 090-175 / 2017)

The applicants requested from the Administrative Court electronic access to applications, defences, preparatory statements and other statements of parties and orders, judgments and other decisions adopted by one of the court departments for a specified period in the past and for the future. The body denied the access claiming that the applicants abused their right of access to public information. The request referred to 792 court files, representing 10,407 pages, and the body made an estimation of how many employees should be involved in preparing the documents to satisfy the applicants' request. The Information Commissioner noted that in the present case, it could be objectively foreseen that if the body considered the substance of the applicants' request, the complex and diverse nature of the documents would impede the performance of tasks the body was primary established; namely, the body could no longer carry out the judicial function by adequately protecting the rights of the parties in court proceedings. Such applicants' request exceeded the legal limit of the right of access to public information, representing an example of the abuse of rights. Thus, the Information Commissioner confirmed the body's decision to refuse the request pursuant to the Para. 5, Article 5 of the ZDIJZ. The Information Commissioner nevertheless emphasized that the criteria for establishing the exemption of the abuse of rights should be interpreted narrowly and on a case-by-case basis.

Copyright material (decision number 090-131/2017)

The applicant requested from the Slovenian Institute for Standardization access to the standard ISO 22716: 2007, Cosmetics - Good Manufacturing Practice (GMP). The body refused the applicant's request because the requested document did not fall within the body's scope of work and it represented copyrighted work. In the complaints procedure, the Information Commissioner found that the requested document does fall within the body's scope of work and represents copyright work. However, since the requested standard is referred to in the EU Regulation and the breach of requirements in the standard constitutes a minor offense under the Implementing Regulation, the required standard is considered as official text. In accordance with Article 9 of the Copyright and Related Rights Act (ZASP), official texts are denied copyright protection. The document must therefore be freely accessible to all citizens as official text. The body is not allowed to charge for the requested standard because it holds the requested documents in electronic form.

Document in the process of being drawn up, classified information, internal operations (decision number 090-258/2017)

The Applicant requested from the Prime Minister's Office access to the current text of the draft amendments to the Slovene Intelligence and Security Agency Act. The body rejected the request and relied on the exception of the document in the process of being drawn up and the exception of internal operations of the body. While the body mentioned in the refusal decision that the requested document was classified as "internal", it did not specifically refer to the exception of classified information. In the complaints procedure, the Information Commissioner first found that there is no reason why the requested document could or should be classified as secret. It further noted that the exception of internal operations of the body cannot be applied, because drafting of statutory text is, by the very nature of things, intended to regulate external and not internal conduct. Therefore, when it comes to drafting laws and regulation that undoubtedly have outward effects, it cannot be claimed that the document relates to internal operations of the body. The Information Commissioner further concluded that the exception of document in the process of being drawn up does not apply, since the requested information was no longer in the production stage, nor was it subject to consultation, and it was already sent externally. The Information Commissioner noted that the public interest in disclosing he requested information might also prevail in this case, reminding of the democratic standard of participation of the public in legislation processes.

Public procurement, business secret (decision number 090-255/2017)

The applicant requested from the Ministry of the Interior access to cost estimates attached to a bid in the call for tenders for the consumable supplies of sanitary materials for the needs of the body. While the body decided to allow access, a third-party intervener filed a complaint against the decision of the body as it disagreed with the provision of information on the manufacturers of the goods on the cost estimates. The Information Commissioner concluded that the information on manufacturers represent the subject-matter of the contract and is therefore information on the use of public funds. This information is essential for determining whether the goods purchased are appropriate and of good quality. The information on the manufacturer of the purchased goods enable the public to learn about the kind of goods the body purchased with public funds and for what price. Only with this information the public can control whether the body used public funds appropriately. The Information Commissioner further found that the exception of business secret does apply to information on the manufacturers on certain document, which were not used as the basis for the conclusion of the contract and thus do not represent information on the use of public funds. In this part, the Information Commissioner refused the applicant's request.

Personal data, civil servants, functionaries (decision number 090-117/2017)

The applicant requested from the Ministry of Foreign Affairs the annual assessment reviews for certain civil servants. The body rejected the request on the basis of the exception of personal data protection in parts that concerned the signatures of civil servants and the reasonings of the assessments. The applicant challenged the decision with regard to the publicity of the reasonings and the Information Commissioner found that they do not contain protected personal data and thus granted the complaint. In the specific case, the reasonings contained only a brief general description of the civil servant's tasks, which makes it impossible to discern personal characteristics of the individual civil servant.

Protection of criminal proceedings, personal data (decision number 090-236/2017)

The applicant requested from the Public Prosecutor's Office access to a criminal complaint and related documents in a specific case. The body rejected the request for access to a criminal complaint on the grounds of the exception of the protection of criminal proceedings and granted partial access to the remaining documents, redacting the reference numbers on the documents due to the protection of personal data. The Information Commissioner found that the body correctly denied access to the criminal complaint, but it upheld the complaint in the part relating to the reference numbers of the requested documents, as it found that they did not represent protected personal data.

Protection of the supervisory proceedings, internal operations of the body (decision number 090-5/2017)

The applicant (journalist) requested from the Motorway Company of the Republic of Slovenia a report of its supervisory board regarding the purchase of certain real estate for the construction of a motorway route. The body refused access on two grounds: the exception of business secret of the body and on the grounds that the Court of Audit of the RS was conducting an audit procedure. The Information Commissioner decided that the requested documents do not represent the business secret of the body, since the body carries out the purchase within the scope of its public-law tasks. It also found that the conditions for the exemption of protection of the supervisory proceedings were not fulfilled because the Court of Audits had not initiated an audit or other supervisory procedure in relation to the specific purchase. However, the Information Commissioner found that the documents contained information on average prices used to calculate the amount of equitable damages in this geographic area, and their disclosure would cause disturbances in operations of the body (the exception of internal operations) and therefore refused access in this regard. The Commissioner allowed access to the rest of the requested information, namely on the purchase in the specific case, the Supervisory Board's opinion on that purchase and the general description of the purchase processes.

Environmental information, business secret (decision number 090-210/2017)

The applicant requested from the Environmental Protection Agency of the Republic of Slovenia access to the audited financial reports of all the schemes on waste electrical and electronic equipment (WEEE) in 2016. The body rejected the request relying on the business secret exception. While the Information Commissioner confirmed the argument that the audited financial statements are marked as business secret, the documents certain information which is public by law. Namely, the Aarhus Convention explicitly included in its "definition" of environmental data information on "cost-benefit and other economic analyses and assumptions used in environmental decision-making", which is exactly what the applicant requested in the present case. In view of the above, the parts of the audited financial reports that contain information on the costs of WEEE collection and handling and the cost of informing, cannot be considered as business as their publicity is prescribed by the Aarhus Convention and the ZDIJZ.

Costs of proceedings (decision number 090-268/2017)

The applicant requested access to certain information and the body attempted to charge him for the costs. The Information Commissioner upheld the applicant's complaint and set aside the decision on costs issued by the body, because the body failed to warn the applicant that he will be charged costs for the provision of public information. Therefore, the body did not comply with the provision of Para. 3, Article 36 of the ZDIJZ. This provision protects the applicant from the costs they are not willing to pay and enables them to change their mind if the body intends to charge for the information. The applicant also has the right to demand that the body informs him in advance of the amount of costs it will charge the applicant. If the applicant is not made aware of the body's intention to charge him, it cannot even verify whether the amount of costs is correct. The obligation of the body to inform the applicant in advance of the costs also indirectly derives from the Regulation on the transmission and re-use of public information.

Classified information, document in the process of being drawn up (decision number 090-194/2017)

The applicant requested from the Ministry of Foreign Affairs access to a diplomatic cable, a part of the supervision report of the Embassy (report) and the draft of this report. The body rejected the request for access to the report relying on the exception of classified information and access to the draft of this report relying on the exception of the document in the process of being drawn up. The Information Commissioner noted that part of the report does not relate to the fields of interest protected by the Classified Information Act (ZTP) which justifies classifying the documents. Thus, the Information Commissioner ordered the body to terminate the classification from the document and provide the applicant with the part of the report in question. However, with regard to the draft report, the Information Commissioner noted that the document is subject to consultation within the body, and its disclosure would lead to a misunderstanding of its contents, which means that the exception relied upon by the body applies. The requested cable contains personal statements of the author, including her personal opinions, in particular regarding the findings of supervision relating to her. Such information is protected personal data as it is not information directly related to the employment relationship of the civil servant or the execution of public functions.

Protection of the administrative procedure (decision number 090-76/2017)

The applicant requested from the Inspectorate of the Republic of Slovenia for Environment and Spatial Planning access to the list of the documents on the inspection file and all documents contained in the said file. The body provided the applicant with the list of documents on the file and denied access to documents as such, relying on the exception to the protection of the administrative procedure. The Information Commissioner dismissed the applicant's complaint as unfounded, as the body duly demonstrated the damage that could occur to the inspection procedure if the requested documents were disclosed to the public. The applicant's allegations that the body should take into account that she was also the party to that procedure are not relevant, because different statuses of applicants cannot be considered in the procedure under the ZDIJZ and no special treatment or privileged position is allowed. The Information Commissioner also concluded that in the complaints procedure the applicant is not allowed to broaden the scope of his or her request for documents, neither is the applicant entitled to request clarifications and answers to questions under the ZDIJZ.

2.3 GENERAL ASSESSMENT AND RECOMMENDATIONS IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

In 2017, the Information Commissioner received 522 complaints in the area of access to public information, which is more than the year before when it received 514 complaints. 321 complaints were against rejection decisions (a year before there were 316 such complaints made), 201 complaints against the administrative silence of the body (198 in 2016) and 7 complaints against business entities under the dominant influence of public bodies. The applicants and liable bodies made 324 written requests for an opinion or clarification (a year before there were 308 such requests). In total, the Information Commissioner handled 853 cases in the area of access to public information (822 cases a year earlier).

The Information Commissioner issued 316 decisions in complaints cases against rejection decisions, more than the year before when it issued 312. The Commissioner endeavoured to resolve the complaints swiftly and without undue delay for the applicants. The average time for resolving the complaints against refusal decisions with special examination procedure required was 37 days. The complaints were thus resolved much more quickly than within the statutory two-month time-limit for resolving such matters laid down in the General Administrative Procedure Act. By comparison, in 2016, the average time of resolving the complaints was 47 days, which means that the Information Commissioner reduced the time for resolving complaints by 22%.

The Information Commissioner notes that in 2017, the number of complaints with regard to the administrative silence is comparable to the number of such complaints in 2016. However, the number of complaints against rejection decisions slightly increased. With regard to the structure of the bodies liable against whom the decisions were appealed, the number of complaints filed against state bodies increased significantly (in 2016, these were 128, and in 2017, 156), while the number of complaints against the municipalities

decreased. In 2017, the Information Commissioner received 41 complaints against municipalities, which is 13% less than the year before. According to the Information Commissioner, this data arguably demonstrates a better management of municipalities in this area in 2017, especially in comparison to previous years when showed a much lower response rate of municipalities in access to information procedures. Also, the number of requests for clarifications and opinions from bodies liable increased again. All of the above shows that bodies liable were more active and responsive in 2017 than the year before, also due to the fact that they contacted the Information Commissioner even outside the complaints procedures.

In 2017, the Information Commissioner handled 7 complaints against the business entities subject to dominant influence, which is much less than the year before, when there were 22 such complaints filed. This is an exceptionally low percentage of all complaints (1.3%), which is why the Information Commissioner believes the situation with regard to the new bodies liable has "stabilized" after the entry into force of the Amendment ZDIJZ-C and that these bodies liable have not been overburdened by the implementation of this law. The Information Commissioner noted a similar situation in 2016.

The Information Commissioner dealt with several important cases as to their substance matters in the complaints procedure. With regard to the exceptions invoked by the bodies liable, it should be noted that there was an increase in the number of cases concerning the so-called "abuse of justice" exception. While in 2016the Information Commissioner handled 13 such cases, there were as many as 29 in 2017. Only in one of these cases, the Information Commissioner confirmed the body's decision and found the abuse of rights, while in all others the bodies liable wrongfully claimed the abuse of rights exception. The Information Commissioner emphasises that this institute should be used as a last resort that may only be invoked by the bodies liable in exceptional cases. This is because the right to access to public information as a fundamental human right should only be restricted for the protection of legitimate interests and rights of others and the restriction should be kept at such minimal level that the protection of such interests of others is still guaranteed. The body claiming the abuse of rights shall demonstrate in a concrete manner that the applicant, with one or more functionally related requests, has clearly abused the right of access to public information or if it is obvious that the request or requests are of a harassing nature. The abuse of rights exception is only applicable where the applicant crosses the boundaries (with a harassing request) of the legally guaranteed entitlement in a way that threatens or interferes with the rights of others.

The data indicates that in 2017, the structure of the applicants who appealed to the Information Commissioner partly changed. In this year too, the highest number of complaints were filed by natural persons (211), which is more than the year before (172). The number of complaints by private legal entities (65) decreased, while the number of complaints filed by journalists (33) remained for the most part the same. It is interesting to note that the number of complaints involving legal entities of the public sector (7) increased, indicating that the right to access to public information is an institute that allows various categories of applicants to obtain information quickly and efficiently. In view of the increasing number of complaints, it can be concluded that applicants are well aware of the access to information procedure and that this procedure is fast, efficient and cost-free.

With regard to the re-use, the Information Commissioner handled three complaints procedures in 2017, which is comparable to the previous year. The Information Commissioner estimates that the applicants, i.e. potential re-users, are well aware of their legal options when faced with a refusal decision, but they do not often decide to use the complaint procedure. Since the entry into force of the amendment ZDIJZ-E, the principle of proactive publication of information applies in the field of re-use of public information. In practice, this principle is implemented through the publication of information through the Open Data Portal managed by the Ministry of Public Administration. In this way, the potential re-users can obtain such open data swiftly and without special procedural requirements, to which the Information Commissioner is bound in the complaints procedure under the ZDIJZ and ZUP.

3 PERSONAL DATA PROTECTION

3.1 THE CONCEPT OF PERSONAL DATA PROTECTION

In the Republic of Slovenia, the concept of personal data protection is based on the provisions determined by Article 38 of the Constitution, according to which personal data protection is among the constitutionally guaranteed human rights and fundamental freedoms. The ZVOP-1 is an organic law that has been valid since 1 January 2005, while the amended ZVOP-1[1] was adopted in July 2007. The purpose of organic laws is to define in a uniform manner general rights, obligations, principles, and measures by means of which unconstitutional, illegal, and unjustified interferences with the privacy and dignity of individuals in the processing of personal data are prevented. Therefore, sectoral laws must clearly determine which filing systems will be established and maintained with regard to individual fields, the types of personal data that individual filing systems will contain, the manner of personal data collection, the possible limitations of the rights of individuals, and, above all, the purpose of processing the collected personal data. With regard to Part VI, the ZVOP-1 is also a so-called sectoral law which by means of the exact definition of rights, obligations, principles, and measures provides data controllers with a direct legal basis for personal data processing in the field of direct marketing, video surveillance, biometrics, recording the times of persons entering and exiting buildings, as well as professional supervision. Furthermore, what is also used in Slovenia are the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention was ratified in 1994[2].

3.2 ACTIVITIES IN THE FIELD OF PERSONAL DATA PROTECTION IN 2017

The Information Commissioner conducted 655 inspection procedures in 2017 for the suspected violations of the provisions of the ZVOP-1, of which 226 pertained to the public sector and 429 to the private sector. It received 189 complaints against public sector legal entities, on the basis of which it initiated 103 inspection procedures, while it initiated 33 procedures ex officio; furthermore, it received 370 complaints against the private sector and upon such basis initiated 196 procedures, while it initiated 59 procedures ex officio. Within the framework of inspection procedures, 28 physical inspections and 6 inspection of webpages were carried out in the public sector, while there were 76 physical inspections and 30 inspection of webpages in the private sector.

With regard to complaints, the largest number of suspected violations of the provisions of the ZVOP-1 referred to the following:

- Unlawful disclosure of personal data; the transfer of personal data to unauthorised users by data controllers and unlawful publication of personal data (174 cases);
- Unlawfully collecting or requiring personal data (98 cases);
- Abuse of personal data for direct marketing purposes (75 cases);
- Unlawful video surveillance (57 cases);
- Inadequate security of personal data (59 cases);
- Processing personal data contrary to the purposes for which they were collected (36 cases);
- Unlawful access to personal data (34 cases);
- Cookies (3 cases);
- Other (88 cases).

In order to redress the established irregularities, the Information Commissioner issued a total of 141 measures (50 in the public and 91 in the private sector) in the form of warnings on the record, preliminary decisions and regulatory decisions.

In 2017, 105 offence procedures were initiated due to violations of ZVOP-1, of which 44 were against public sector legal entities, 27 against private sector legal entities, and 34 against individuals. In offence procedures in 2017 the Information Commissioner issued 10 warnings and 93 decisions regarding violations (44 cautions and 49 fines). Furthermore, the Information Commissioner issued 70 warnings for minor violations. Violators filed ten requests for judicial protection against the decisions issued.

[1]Official Gazette RS, No. 86/2004; hereinafter: the ZVOP-1.
[2]Official Gazette RS, No. 11/1994 – International contracts no. 3/1994.

In 2017, the Information Commissioner received 11 judgments whereby local courts decided on requests submitted for judicial protection against decisions by the Information Commissioner regarding offences. The decision of the Information Commissioner was upheld in 7 cases, the sanction for the offender was changed in 3 cases, and in one case two misdemeanours joined in one, while the sanction remained unchanged.

In 2017, the Information Commissioner issued 1.289 written explanation and referrals to the already published opinions. Most opinions are published on the following website: www.ip-rs.si. Furthermore, the Information Commissioner issued opinions and explanations over the telephone. In 2017, the State Supervisors received 1,998 calls and the Information Commissioner gave advice to almost 3.300 individuals all together.

In 2017, the Information Commissioner received 4 requests on the permissibility of implementing biometric measures and issued 1 decision in this regard. In this case, the Information Commissioner partially allowed the use of the fingerprint scanner of the employees authorized to enter the premises of the radiographic laboratory. The Commissioner based its decision on ensuring safety of people, as unauthorized entry into the laboratory and removal of radioactive materials from it could have very serious consequences for the wider environment or the life and health of the general population. However, the applicant's request was rejected by the Information Commissioner in so far as it concerns individuals who are not employees, because such a measure is not allowed by the law.

In 2017, the Information Commissioner received 29 applications for the transfer of personal data out of the Republic of Slovenia. It issued 34 decisions (6 for the applications filed in 2016) and permitted the following transfers of personal data:

- 25 companies were allowed transfer of personal data to their processors in the USA, India, Australia, Serbia, United Arab Emirates, Turkey, Morocco and the Philippines for the purposes of using cloud services, conducting clinical trials, human resource management, IT system development etc.;
- 8 companies were allowed transfer of personal data to other data controllers in the USA for the purposes of human resource management, production of statistical and other data, customer relations management, etc.;
- One company was allowed to transfer personal data within international group companies for the purposes of conducting research and other production needs, ensuring healthcare services, commercial purposes and for the purpose of ensuring corporate support.

A large number of applications is a result of the decision of the Court of the European Union in October 2015 in the Schrems case and consequently of the annulment of the so-called Safe Harbor agreement which represented the basis for the controllers to transfer data from the EU (also from Slovenia) to the USA. Because the Information Commissioner is bound by the decision of the competent EU body on the adequate levels of data protection, the Commissioner annulled its decision from 2010, by which it has found that the USA ensures an adequate level of data protection when data is being transferred by organisations that adhere to the Safe Harbor principles. The controllers thus needed to file new applications for the transfer of data to the USA. In March 2017, the Information Commissioner, upon the decision of the European Commission, listed the USA as a third country which guarantees adequate level of data protection, in part that relates to data transfer in the framework of the EU-US Privacy Shield.

In 2017, the Information Commissioner received 16 requests from data controllers to link with another or other personal data filing systems and in 12 cases it permitted the linking of filing systems. For example, the Information Commissioner permitted the Office for Money Laundering Prevention to link their registers with the Central Population Register, whose controller is the Ministry of the Interior, and the Real Estate Register, Land Cadastre and Building Cadastre, whose controller is the Surveying and Mapping Authority of the Republic of Slovenia. Another example of permitted linking includes the linking of Driving Licenses Records, managed by the Ministry of Infrastructure, with the Passport records, Identity card records and the Central Population Registers, whose controller is the Ministry of the Interior.

In 2017, the Information Commissioner received 110 appeals regarding the right to access to one's personal data, which is more than in the previous year (91). The appeals filed concerned state authorities, ministries, and constituent bodies (40 cases), health care institutions (21 cases), educational institution (11 cases), Social Work Centres (10 cases) and various other controllers. The Information Commissioner issued 11 decisions, whereas it granted the appeal in two cases fully and in five cases partially and issued four decisions rejecting the appeal. The Information Commissioner transferred five appeals to competent authorities for

consideration and rejected three appeals on procedural grounds.

In 2017, the Information Commissioner filed one request for a review of the constitutionality to the Constitutional Court of the RS and assisted the Slovenian Ombudsman in another request for a review. The first concerned the constitutionality of the Slovene Intelligence and Security Agency Act (ZSOVA). Namely, Article 21 of the ZSOVA provides that the Director of the Agency may authorize the monitoring of international communications systems and the covert purchase of documents and objects by a written order. The Information Commissioner believes that such authorisation bestowed upon the Director of SOVA is contrary to the Constitution of the Republic of Slovenia, as the Constitution requires that such interferences with privacy are approved by the court. Furthermore, the conditions and circumstances for interfering with the privacy of individuals are not clearly defined, and the contested article of the ZSOVA is also contrary to Article 8 of the European Convention on Human Rights. In the second case, the Information Commissioner warned about the alleged unconstitutionality of the amendment of the Law on Police Tasks and Powers (ZNPPol-A) but was barred from filing a request for a review of constitutionality due to the specifics of the procedure before the Constitutional Court. Instead, the Commissioner suggested to the Ombudsman of the RS to file a request and assisted with its expertise. The Commissioner was worried because the ZNPPol-A allowed the implementation of biometric measures in a generalised way, collection of data on all airline passengers, optical license plate recognition and the use of drones. According to the Information Commissioner, these measures are implemented without adequate safeguards, disproportionately and without discrimination interfere with the rights and freedoms of individuals and introduce mass surveillance that is left to the discretion of individual police officers.

3.3 SELECTED CASES OF PROCESSING OF PERSONAL DATA

The Information Commissioner presents ten notable decisions, adopted in proceeding conducted in 2017.

Inadequate security of documentation intended for destruction

The Information Commissioner received a report that there are several medical prescriptions lying around in the vicinity of a certain warehouse and initiated an inspection procedure against the owner of the warehouse in question due to the suspicion of inadequate personal data security. The Data Protection Supervisor inspected the liable entity's premises, received information on the process of taking over and destroying wastepaper, and seized several prescriptions as evidence. It was discovered that there were several deficiencies with the process of confidential information destruction and as soon as the liable entity became aware of this it changed the procedure. In accordance with the provisions of the ZVOP-1, the liable person was a data processor for the pharmacy, so the Information Commissioner also instituted an inspection procedure against the pharmacy as the data controller. The Information Commissioner noted that the pharmacy ordered the data contractor in writing to destroy personal on the basis of a purchase order, but they had not concluded a contract for the processing of personal data. The Information Commissioner imposed a fine on the liable entity for failure to secure personal data and a warning on the pharmacy as the data controller.

Collecting personal data of payers

The Information Commissioner received several reports that Pošta Slovenije, d. o. o., collects personal data of the payers of bills or the recipients of packages paid for upon delivery. It was found that the amended Regulation (EU) No 2015/847 on information accompanying transfers of funds entered into force in Slovenia in June 2017. The Information Commissioner determined that there was no violation of ZVOP-1, since the person liable processed personal data on the basis of personal consent and for acceptable purposes. The Information Commissioner therefore stayed the inspection procedure.

Unlawful disclosure of pupils' personal data

During the inspection procedure, the Information Commissioner found that the elementary school teacher kept a list of pupils in relation to the payment of fine art material and that she obtained pupils' personal data from official records from a school counsellor. The latter sent a file with personal data of all pupils (their surnames and first names, dates, countries and places of birth, personal identification number, residence addresses and birth certificate numbers) to all teachers at the school. The teacher then sent a list with

payments, containing pupils' personal data, to the headmaster, who forwarded it to the representative of the parents' council, who then forwarded it to all the parents of pupils from the class in question. The Information Commissioner found that these actions were not in accordance with the lawful purposes and without the legal basis in law or personal consent of individuals. In the minor offence proceedings, the Commissioner fined the headmaster and issued a warning to the teacher for using personal data from the official record to compile a list and to the school counsellors for sending an e-mail with personal data of all the pupils from the school.

Unlawful processing of personal data in police records

Within the internal control process, the Police found that some of its employees with an authority to access personal data files for the purposes of performing their duties and tasks processed personal data contrary to the purposes for which they were collected. The Police filed a report with the Information Commissioner with relevant evidence, i.e. the access logs and employee statements regarding the purpose of personal data processing. The Information Commissioner found that violators used their personal passwords to access specific reports on the work carried out by a particular police station and, in that document, a specific event that contained personal data of certain individuals. The Information Commissioner found that the violators did not have any legal basis for such processing of personal data as they did not need such information for any official purposes, namely in the course of performing their duties and tasks. The Information Commissioner has imposed fines on all violators for the minor offences, which it always does in cases that involve the use of personal data from official records for private purposes (most often as a matter of curiosity) and the use of data that the violator had access to in the course of their work.

Unlawful sending of employee's personal data to the members of the federation

In the inspection procedure, the Information Commissioner found that a certain employee, by order of the president of the federation, sent 154 members of the federation (namely, the societies) an email about irregularities in the work of an employee, accompanied with travel orders, a copy of the decision on the annual leave and a copy of the payroll of the employee with the following personal data: the name, address, tax number, duration of the service and the account number. The Information Commissioner found that the liable entity had a legal basis for sending unsigned payment orders and a payment order with a forged signature, with the employee's address, because the members of the federation have the right to be informed about the work of the liable entities working bodies and about any irregularities detected. However, there was no legal basis for sending via email the copy of the employee's payroll, which resulted in the Information Commissioner imposing a fine on the violator.

Publication of personal data of the members of a society on the Internet

In the course of the inspection procedure, the Information Commissioner found that entering certain URL links into a web browser provides unsecured access to a large number of personal data of members of the societies affiliated with the federation. The tables that were published included, among others, the following personal data: names and surnames of the members of the society, e-mail addresses and addresses, dates of birth, mobile phone numbers and telephone numbers, as well as the membership card numbers. The liable entity immediately after the Information Commissioner called to intervene took off the personal data published from the website. The liable entity explained that access to the website had been unsecured for some time due to extensive testing of the transfer of membership data from one information system to another. Due to inadequate security of personal data, the Information Commissioner issued a warning to the liable entity, whereas it issued a fine on the external service provider who failed to provide measures for securing personal data of a large number of individuals (around 500) on the liable entity's web server and thus failed to prevent unauthorized processing of personal data.

Publication of documents with personal data of witnesses in minor offence proceedings on websites

The Information Commissioner found that the liable entity published a large number of personal data of violators and witnesses as part of a news article in the form of photographs of official documents (indictment, summons to the accused). While the liable entity possessed with a written consent of the accused to publish

his personal information, it did not have the consent of the witnesses. The Information Commissioner determined that in the absence of a legal basis for the processing of personal data, the liable person should redact such documents prior to their publication, which it failed to do. As the publication of personal data on the Internet is one of the most serious forms of violations of the right to the personal data protection, the Information Commissioner imposed a fine on the person liable for inadequate security of personal data.

Inadequate protection of the file structure of a notary office

During the inspection procedure, the Information Commissioner found that the notary's file structure with all the documents was freely accessible on a certain website, without any specific protection, which made it possible to process all personal data in the files: names, surnames, dates of birth, residence addresses, personal identification numbers, information form the identification documents, bank account numbers, data on ownership and value of real estate, kinship ties and other circumstances of family life of individuals. The Information Commissioner called the liable entity over the telephone and urged it to correct the irregularities, which the liable entity did on the same day. The liable entity explained that an external service provider maintained their information infrastructure on the basis of a contract. The Information Commissioner instituted an inspection procedure against the data processor and found that the latter did not provide an adequate level of security of personal data, regardless of the fact that the service provider relied on a hacking attack on the information system.

Collecting data on reasons for sick leave

During the inspection procedure, the Information Commissioner found that the employer had adopted the Policy on Reduction of Sick Leave (Policy), which provides for the collection of personal data on the health status of employees. The Information Commissioner noted that in principle the personal consent of employees as the legal basis for personal data processing, on which the liable entity referred to, is excluded in the employment relationship because the employee is in a subordinate position and there is a clear imbalance of powers between the employer and the employee. The consent can be the basis for processing of personal data in employment relationships only in rare situations, for certain voluntary, additional activities or processes that the employee may refuse without fear of affecting his employment relationship in any way; thus, when personal data are not processed for the purposes of carrying out the rights and obligations arising from the employment relationship. In the specific case, the Information Commissioner found that the employer had no valid legal basis for the processing of the personal data at issue. It noted that the employer may collect information about the employee's movement regime (doctor's instructions on rest) and the estimated time of absence in relation to sick leave. The employer may obtain information from the employee or his personal physician, who is not obliged to provide the data. The employer is also entitled to obtain information on the reason for temporary absence from work, because it needs it to calculate remuneration during temporary absence but has no legal basis for obtaining a diagnosis with regard to the illness or injury.

Obtaining and publishing surveillance recordings on social media

The Information Commissioner received information that a surveillance recording of a theft from a car parked in a public space was published on Facebook. During the inspection procedure, the Information Commissioner found that the individual obtained a video recording from the liable entity who recorded the entrance on its land parcel, but also covered the road where the car in question was parked. The Commissioner further noted that the liable entity had no legal basis for transmitting the recording to the individual, despite the fact that the recording showed the individual's belongings being stolen. The recording of the theft can be obtained by the Police as a law enforcement agency under the Police Tasks and Powers Act and the Criminal Procedure Act, which in this case did. Furthermore, the individual has the legal basis to obtain the recording from the police as the injured party but is not allowed to post it on Facebook. With regard to the recording of a road which is not owned by the liable entity, the Information Commissioner notes that the video surveillance operator may also capture a part of the public road if this is absolutely necessary so that the private space can be monitored to fulfil the purposes of video surveillance (e.g. securing the property, entry and exit controls). This inevitably means that the images of passers-by are also captured, which represents an interference with their privacy. Therefore, the Information Commissioner adds that the liable entity may only access the recordings for the purposes specified by the ZVOP-1. This means that in the event of an incident (such as damage or theft), the controller may access the video archive, but must adequately record any such access and is not allowed to monitor live image.

3.4 GENERAL ASSESSMENT OF THE STATUS OF PERSONAL DATA PROTECTION AND RECOMMENDATIONS

In carrying out the inspection proceedings, the Information Commissioner handled:
- 655 inspection cases, of which 226 were in the public sector and 429 in the private sector, and
- 105 minor offence proceedings.

In addition to inspection and minor offence procedures, the Information Commissioner in 2017 received and dealt with:
- 1,289 requests for written opinions and clarifications in the field of personal data protection,
- 16 applications for permission to connect filing systems,
- four applications for permission to implement biometric measures,
- 29 applications for permission to transfer personal data,
- 110 complaints against the refusal of access to personal data.

Of the 655 inspection cases that the Information Commissioner handled in 2017, 559 were initiated on the basis of a report, and 96 were initiated on the Commissioner's initiative. In the public sector, 189 reports and complaints were filed and in the private sector 370. The number of reports on suspicion of violations of personal data protection rules has been comparable to previous years. Similarly as in previous years, a prevailing number of reports concerned the supply of personal data to unauthorised recipients, unlawful collection or requiring personal data, the use of personal data for the purposes of direct marketing (in particular, unlawful obtaining of personal data for these purposes and disregarding the individual's request for data controller to no longer use personal data for these purposes), the implementation of video surveillance systems and unlawful use of video recordings (in particular, in work areas), the inadequate security of personal data, the use of personal data contrary to the purposes for which it was collected and for unlawful accessing to personal data.

As in the previous years, the Information Commissioner found in 211 out of 559 examined reports (39% of the reports received) that it is possible to conclude from the statements in the report alone that the reported conduct does not constitute such a breach of the provisions of the ZVOP-1 which would fall under the Commissioner's competences. The main reason for such a high number of unsubstantiated reports is that applicants lack knowledge of the regulations in the field of personal data protection and the powers of the Information Commissioner. Unfortunately, the Information Commissioner all too often receives reports that are not intended to protect the public interest or to establish a legal state of affairs in the field of personal data protection, but may derive from vexatious reasons, the desire for revenge, attempts to resolve mutual disputes and pursue private interests that are impossible to pursue in the Commissioner's inspection procedures. A large number of unfunded reports and the need to pursue them hinder the performance of the so-called preventive inspection control in fields where it should be even more intense. The State Supervisor who carries out the inspection sends a written notice to persons who filed a report, providing the reasons why the described conduct does not constitute a violation of the law or for which the Information Commissioner is not competent to act. However, the applicants often file a complaint against such notifications and push for the Commissioner's actions.

Unfortunately, there are still big problems with entities liable who do not have business premises but operate only "through" a mailbox and entities liable that registered a foreign national as the responsible person in the Business Register. In the majority of cases they engage in online sales and collect and use personal data for intrusive direct marketing.

It is worth noting that there was an increase in the number of reports due to unlawful collection or requesting of personal data, which was largely due to the lack of or inadequate information given to data subjects. During the inspection proceedings, the Commissioner often found that while there was an adequate legal basis for collecting the requested personal data, the controllers failed to provide data subjects with the appropriate information on the purpose of the data collection, which made them reasonably suspected that the controller had no legal basis for the collection of personal data and filed a report to the Information Commissioner. When obtaining personal data, the data controller must, in accordance with the provisions of Article 19 of ZVOP-1, provide the individual with the following information: on the data controller and its address or seat, the purpose of processing and other information, if necessary, to ensure lawful and fair

processing (information on recipients of personal data, information on whether the collection of personal data is compulsory or voluntary, and on the possible consequences if the individual does not provide data voluntarily, and information on the right to access, transcribe, copy, supplement, correct, block and erase personal data). The new European General Data Protection Regulation, which comes into effect on 25 May 2018, is even stricter with regards to information to be provided to the individual before processing personal data obtained directly from the individual. Namely, Article 13(2) and (3) provide for a much broader set of information to be provided to the individual than the ZVOP-1.

In addition to handling the reports, the Information Commissioner also strengthened the implementation of the so-called planned ex officio inspections in areas where, according to the risk assessment, there was a greater likelihood of violations of personal data protection legislation or there is a danger of greater harmful effects for data subjects due to the sensitivity of data processing. In carrying out such extensive or more thorough inspections, the Information Commissioner gives special attention to examining and ensuring information security, which is aimed at preventing unauthorized processing of personal data and accidental or unauthorized destruction or loss of personal data, carried out annually in accordance with the annual plan. In 2017, the planned supervision of compliance with the provisions of the ZVOP-1 was performed in ministries, administrative units, health institutions, major data processors, tourist agencies, trade unions and their federations and associations and their federations.

Similar to previous reports, the Information Commissioner notes that the awareness of both the general public and the professional public regarding privacy and the protection of personal data has improved significantly and is still improving. The main problems with knowing the legislation have been superseded, but the Commissioner still observes certain deficiencies and irregularities with data controllers and processors in certain areas. Among the most common are irregularities and deficiencies regarding undefined or ill-defined organizational, technical and logical-technical procedures and measures for securing of personal data in internal acts of controllers. In addition, the Commissioner often finds deficient or inadequate internal and external traceability of processing of personal data, incomplete list of persons responsible for individual filing systems and persons who are authorised to process certain personal data due to the nature of their work. Other irregularities include providing unsuitable or deficient information to data subjects upon the collection of personal data, excessive and disproportionate implementation of video surveillance in the workplace, using recordings for supervising the employees, failing to comply with individuals' request for cessation of processing of personal data for the purposes of direct marketing, deficient contracts with data processors, and redirecting and unauthorised reading of company e-mails.

The Information Commissioner also frequently finds deficiencies in managing up-to-date catalogues of personal data filing systems and consequently of supplying information for the Register of filing systems. In this regard, it is worth noting that the GDPR suspended the Register of filing systems and the current catalogues of data filing systems will be replaced by records of processing activities as provided by Article 30 of the GDPR. The same Article also obliges data processors who carry out processing on behalf of data controllers to keep records of processing activities, while the ZVOP-1 prescribed no such obligation on the processors.

It should be pointed out that the entities liable, as a rule, eliminate the abovementioned irregularities and deficiencies voluntarily on the basis of a warning issued to them by the Data Protection Supervisor. For this reason, issuing a (regulatory) inspection decision is usually not necessary. However, the voluntary elimination of the irregularities found does not relieve the person liable of the offense, criminal and compensation liability.

In 2017, the European region was largely influenced by the preparations for the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR).

The General Data Protection Regulation was adopted on 25 May 2016 and will come into force in all Member States within two years. Larger controllers have already started preparing for the entry into force of the GDPR, while some of the smaller controllers who were, until now, excluded from complying with several provisions of the ZVOP-1 (e.g. establishing filing system catalogues reporting personal data filing systems to the Information Commissioner) were less acquainted with personal data protection legislation. This was reflected in the presentations of the GDPR at conferences, roundtables, consultations and at the event to

mark the Personal Data Protection Day, when a number of issues were raised which did not relate to the rules the future GDPR will bring but to the existing rules under the ZVOP-1 and sectoral laws governing the processing of personal data (e.g. in the field of employment law). A similar situation was noted by the national supervisory authorities of other Member States of the EU. It was proven again that partial exemptions are dangerous, as some liable entities perceive partial exemptions as complete exemptions from the obligation to comply with the data protection rules.

The year 2017 also saw a start of preparations for the new ZVOP-2, which is the responsibility of the Ministry of Justice. With ZVOP-2, the Republic of Slovenia will be able to implement into our legal order certain areas (such as the rules on health, biometric and genetic data), relation to other areas (e.g. to the field of access to public information, freedom of expression, archival, statistical and scientific research activities) and certain procedural aspects (e.g. regarding the exercise of individual rights, minor offences and administrative procedures regarding the protection of personal data) for which the Member States have more leeway when regulating. The Information Commissioner provided comprehensive opinions on draft ZVOP-2 in the public debate.

Designating a data protection officer presents a special challenge for certain data controllers and processors. This institute was already known in practice in larger banks and insurance companies, but now the GDPR imposes an obligation to designate a data protection officer in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

It is crucial that data protection officers have practical experience and knowledge of data protection legislation, and above all, that they are supported by the management, who needs to recognized an internal oversight role of the data protection officer and see that it represents the interests of the organization in terms of reducing the risk of violations of the legislation. Data protection officers have the role to supervise, advise and give information, while the compliance responsibility lays with the management.

Preventive activities

As well as in previous years, the Information Commissioner paid special attention to the preventive aspects of its activities. Aiming to educate data controllers and other liable entities, the Commissioner delivered more than 100 lectures to domestic audiences and issued more than 100 opinions on draft laws and regulations.

In 2017, the Information Commissioner initiated the “Initiative 20i7” in order for data protection supervisory authorities from the former Yugoslavia to join forces, as they face similar professional issues and challenges. As many companies and public sector organizations in the region collect and exchange personal data cross-border, it is vital to ensure appropriate and uniform level of personal data protection also from an economic perspective. The objective of Initiative 20i7 is to foster close cooperation and exchange good practices in the area of personal data protection in the region. Such an initiative in the field of human rights protection can further contribute to strengthening good relations between the countries involved. The first meeting of the Initiative took place in Bled in May 2017.

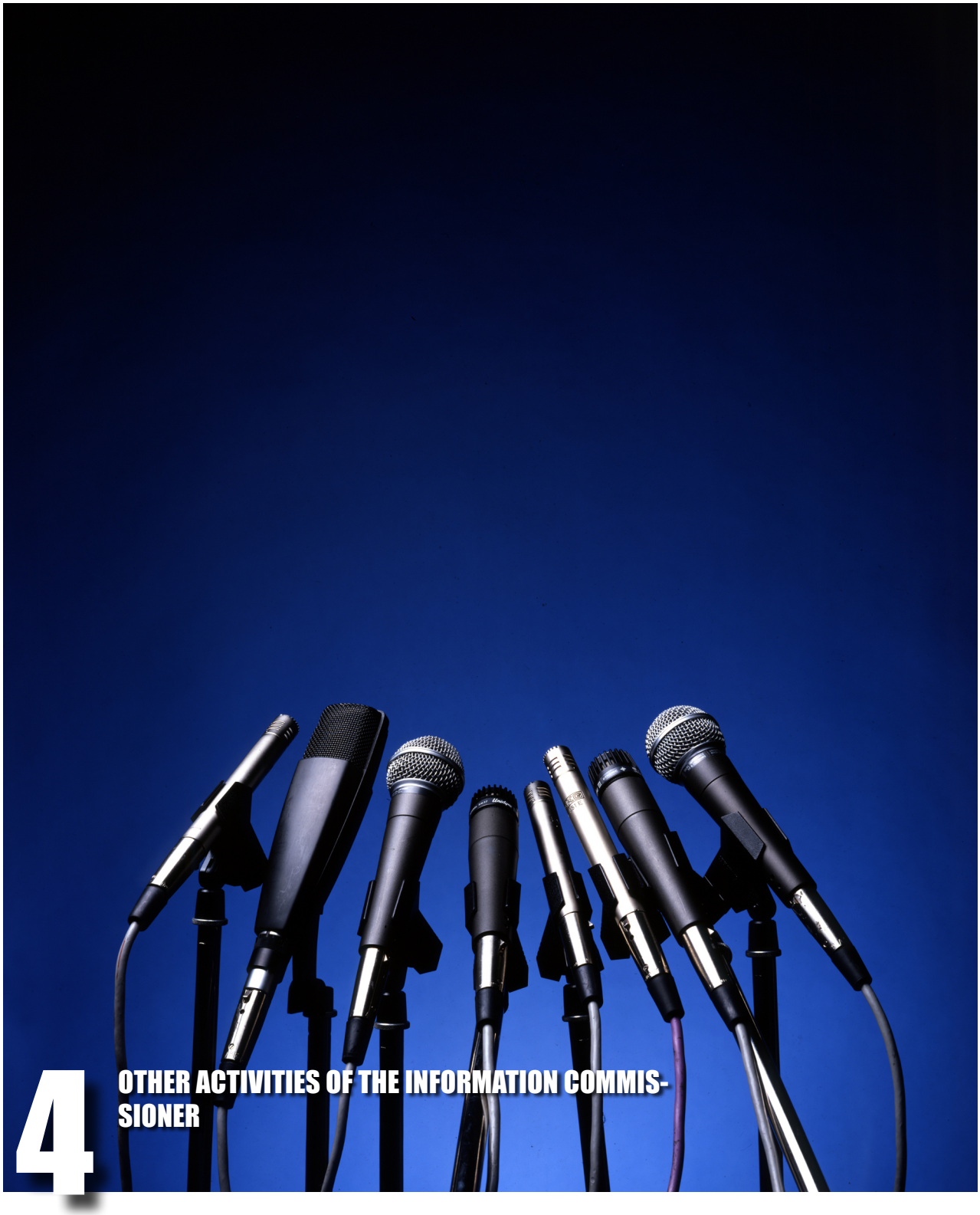
One of the basic preventive tools for timely data protection is also informal personal data impact assessment which the Information Commissioner offers. In 2017, more than 100 public and private sector controllers and processors approached the Information Commissioner when drafting legislation, designing solutions or projects and wanted to consider the risks in a timely manner to avoid violations of the law.

The Information Commissioner also issued new guidelines and guidance for data controllers, namely the Guidelines for Social Work Centres and the first guidelines under the GDPR - the Guidelines on Personal Data Impact Assessment. In order to raise awareness of the GDPR, the Information Commissioner opened a special tab on its website, where it publishes its own materials and links to opinions and guidelines that it prepares in cooperation with information commissioners from other countries within the Article 29 Working Party. In the light of the forthcoming General Data Protection Regulation, the Article 29 Working Party Guidelines on

consent and the Guidelines on Data protection officers are of particular importance.

The Information Commissioner's preventive activities also spread to professional cooperation in interdepartmental expert groups, such as the Inspection Council, the Interdepartmental expert group on eIDAS Regulation on Electronic Identification, cooperation in drafting regulations, cooperation with the Ministry of Public Administration on various eGovernment and digitization projects, and participation in the Council of Informatics Development.

The Information Commissioner's Experts raise awareness of the importance of privacy and personal data protection by participating in various conferences, expert events, consultations and round tables. At the end of the year, the Information Commissioner, in cooperation with the Consumer Association of Slovenia, applied for an EU project on raising awareness of small and medium-sized enterprises and the general public about personal data protection as part of the two-year project Raising Awareness on Data Protection and the GDPR in Slovenia - RAPID.SI. The project is scheduled to begin in July 2018.



4 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

4.1 PARTICIPATION IN THE PREPARATION OF LAWS AND OTHER REGULATIONS

In accordance with the provisions of Article 48 of the ZVOP-1, the Information Commissioner issues prior opinions to ministries, the National Assembly, bodies of self-governing local communities, other state authorities, and bearers of public authority regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations regulating personal data.

In 2017, the Information Commissioner issued more than 100 opinions in the process of preparation of laws and other regulations, including the following:

- Draft Accessibility of Websites and Mobile Applications Act
- Proposal for Market in Financial Instruments Act
- Proposal for Notary Act
- Proposal for Act Amending the Public Employees Act (three opinions)
- Proposal for Act Amending the Healthcare Databases Act
- Proposal for Rules on the operation of the State Attorney's Office (three opinions)
- Amendments to Central Credit Register Act (two opinions)
- Proposal for Information Security Act (two opinions).

4.2. RELATIONS WITH THE PUBLIC

Throughout 2017, the Information Commissioner provided for the publicity of its work and it raised awareness of legal entities and natural persons by means of regular and consistent contact with the media (by means of press releases, statements, commentaries, interviews with the Head of the Information Commissioner, press conferences) and through its website www.ip-rs.si. The Commissioner was also active on social media, namely on Facebook.

In 2017 the Information Commissioner continued its preventative work and dedicated a great deal of attention to continuing to disseminate tools and aids for raising awareness. It issued the Guidelines for Social Work Centres and the Guidelines on Personal Data Impact Assessment under the GDPR. The Information Commissioner has not been printing its publications for a long time, it only publishes them in an electronic form. All publications are available at https://www.ip-rs.si/publications/guides-and-guidelines/.

In 2017, the Commissioner's employees delivered 132 lectures free of charge for expert public and for liable entities of various kinds in both fields of its activity, i.e. for data controllers (100 lectures) and for bodies liable for providing public information (32 lectures).

The Commissioner takes an active role in the Safer Internet Centre, whose mandate is to create a safe and open internet environment for children.

On 28 January 2012 the Information Commissioner marked the European Personal Data Protection Day by organising a conference entitled Individuals' rights and controllers' duties in accordance with the new EU General Data Protection Directive. As has become a tradition, on this occasion the Information Commissioner awarded prizes for good practice in the area of personal data protection. The private sector controller who received the award was Elektro Ljubljana and public sector controller was Primary school. A special award "Privacy Ambassador" was received by the company TIBOPO, d. o. o., for its approach to developing an information system for improving road safety. Awards were also received by companies which in 2016 became certified in accordance with the ISO/IEC 27000 information security management standard and thus demonstrated a high level of personal data security.

Every year on 28 September the International Right to Know Day is marked. On this occasion organizations from all over the world emphasise the importance of the fight for transparency and accountability of the public sector and of ensuring efficient participation of citizens. In 2017, the Information Commissioner dedicated that day to the transparency of spending public funds; the event was entitled "Monitoring the use of public funds – My right to know". The Information Commissioner invited to this event state representatives and civil society representatives, who presented different views on issues surrounding this topic. The Information Commissioner also granted the Ambassador of Transparency Award for good practice in the area of access to public information. The recipient of the award was the Administration of the Republic of Slovenia for

Food Safety, Veterinary and Plant Protection, which in recent years proved its commitment to transparency, including by proactively publishing its public information. The widespread publication of information and findings from inspection proceedings (e.g. from inspecting the operations of the bakeries, catering facilities and beekeepers) can serve as an example to other inspection bodies.

4.3. INTERNATIONAL COOPERATION

As the national supervisory authority for the protection of personal data, the Information Commissioner cooperates with the competent bodies of the European Union (EU) and the Council of Europe engaged in personal data protection.

In 2017, the Information Commissioner actively participated in seven EU working bodies engaged in supervision of the implementation of personal data protection within individual areas of the EU, namely the following:

- The Article 29 Working Party for personal data protection, as well as in four of its subgroups (Cooperation, Technology, E-government and Future of Privacy);
- The Europol Joint Supervisory Body, or, from May 2017, the newly established Europol Cooperation Board;
- The Joint Supervisory Authority for Customs;
- At co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of SIS II;
- At co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of CIS;
- At co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of VIS;
- At co-ordination meetings of the European Data Protection Supervisor (EDPS) together with state national authorities for the protection of personal data (EURODAC);

The Information Commissioner also regularly participated in the International Working Group on Data Protection in Telecommunications (IWGDPT). Once again in 2017, a representative of the Information Commissioner participated in the Council of Europe's Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

In 2017, the Information Commissioner initiated the Initiative 20i7 in order for data protection supervisory authorities from the former Yugoslavia to join forces, as they face similar professional issues and challenges. At the first meeting of the Initiative, held in May 2017 in Bled, Slovenia, the representatives of data protection supervisory authorities from Croatia, Serbia, Bosnia and Herzegovina, Montenegro, Kosovo, Macedonia and Slovenia discussed the implementation of new EU data protection standards, personal data protection in the telecommunication sector and efficient supervision of personal data in the law enforcement sector.

In 2017, the Information Commissioner hosted representatives of similar institutions from Turkey and Macedonia to whom it presented its activities and good practices in its fields of competence.

The Information Commissioner answered 98 questions and questionnaires from data protection authorities from abroad, international organizations, academic and research institutions and non-governmental organizations from abroad.

In the period from 2014 and 2017, the Information Commissioner cooperated in CRISP project which aims to develop a new scheme for certification of security products and services, such as (smart) video surveillance systems, security information solutions, biometric solutions, body scanners, etc. The project successfully concluded in April 2017.