Information Commissioner of the Republic of Slovenia

'16

Annual report

The Annual Report 2016 on the activities of the Information Commissioner shows that this was a crucial year for the Information Commissioner, both due to the changes in legislation, as well as due to the volume of activities and the number of cases that it dealt with. The Commissioner issued more than 312 decisions on complaints in the field of access to public information, which is the largest number since the beginning of its work. In the field of personal data protection, the Commissioner dealt with 683 inspection cases, its employees prepared more than 1330 written opinions and gave advice over the phone to individuals, companies and other organizations on more than 2500 inquiries.

In 2016, the field of personal data protection was marked by the adoption of the European Union regulatory package, namely by the reform of personal data protection. This reform was a pivotal step for the whole of the European Union, as data controllers received a number of new obligations, individuals were afforded new rights, and the Information Commissioner was tasked with new duties and responsibilities. The field of access to public information was marked in particular by the amendments to the Access to Public Information Act (ZDIJZ-E), which implemented the amended European directive on the re-use of public sector information. Its purpose is to provide everyone with the right to easy and effective re-use of public sector information for any purpose. Therefore, from May 2016, museums, libraries and archives are also included in the regime of re-use of public sector information, but only in relation to materials that are freely available and to which no third party is entitled to intellectual property rights.

In order to maximize the impact on the rights of individuals, the Information Commissioner focused in 2016 on educational activities, swift handling of complaints in the field of access to public information and effective actions against violations in the field of personal data protection. A guiding principle of the Commissioner is to identify the key areas in a timely manner (based on the received complaints, reports, and ex officio inspections), where we can best assist individuals in exercising both constitutional rights. When it comes to the protection of personal data, our priority is to quickly resolve urgent matters where there is a likelihood that a larger number of individuals will be affected and where sensitive personal data are involved. This means that such cases have priority, in terms of the speed and urgency of our response, over the individual reports, where privacy is no longer threatened.

In the field of access to public information, the Information Commissioner received 514 complaints in 2016. Of those, there were 316 complaints against the rejection decisions and 198 complaints against the silence of the body. We are pleased that the number of complaints due to the silence of the body has dropped significantly, however, the number of requests for opinions and explanations increased. This shows that the bodies liable were more active and responsive this year than the year before. The average time for resolving the appeals against rejection decisions, in which a special declaratory procedure is required, was 47 days, which proves that the Commissioner's efforts to resolve complaints as soon as possible already yielded results. Most of the complaints challenged rejection decisions of State bodies, but there were nevertheless fewer such complaints than the year before. We noticed again an increase in complaints against rejection decisions of municipalities.

In 2016, as in previous year, the Commissioner noticed an increase in complaints in the area of access to environmental information. The Slovenian legislation sets the highest level of transparency precisely for environmental information and there is virtually no legal exception possible for free access to such information.

We note that the expectations of the public regarding the efficient use of modern technologies in the public sector are also reflected in the complaints in the field of access to public information. Thus, in the year 2016, the majority of complaints did not concern the exception of personal data protection (as before, several years in a row), but the question whether the requested information even exists. In times of rapid information technology developments, the applicants expect from the bodies liable that they hold various statistical data and that their information is searchable according to different criteria. However, the practice often paints a different picture. The Information Commissioner therefore welcomes the solution implemented by Article 10b of the Amendment ZDIJZ-E. Namely, the legislator ordered the bodies liable to proactively provide open data for the re-use by publishing data on the Internet and on the Open Data Portal. Indirectly this ensures a significantly higher level of transparency.

In the field of personal data protection, the Information Commissioner performed its functions in relation to inspection and minor offences procedures, issued opinions and handled requests to connect filing systems

and to implement biometric measures. In addition, it handled as many as 53 applications for authorisation for the transfer of personal data to third countries and 91 complaints from individuals for having been refused access to their personal data.

The number of reports on suspicion of violations of legislation in the field of personal data protection received by the Information Commissioner in 2016 was similar to previous years. The largest share of reports concerned the transfer of personal data to unauthorized users, the implementation of video surveillance (especially in the workplace), reports on the use of personal data for the purposes of direct marketing (in particular due to the suspicion of unlawful acquisition of personal data for these purposes and the failure to respect the individual's prohibition of the use of personal data for these purposes), redirection and consequent reading of e-mails addressed to the official e-mail address of employees, the publication of personal data on websites and the lack of measures to protect personal data. With a view of ensuring the highest possible level of protection for all residents of Slovenia, the Information Commissioner in 2016 increased the activities related to the so-called planned ex officio inspections, which are carried out each year in accordance with the adopted annual plan. Such planned supervision of compliance of the provisions of the ZVOP-1 were most frequently conducted in 2016 at the police, health institutions, banks and savings banks, with consumer creditors, insurance companies, local self-government bodies, higher education institutions, secondary schools and energy companies.

As we have already noted in the 2015 Annual Report, over the last ten years of the Information Commissioner's activities, the awareness of both the general and the professional public regarding privacy and data protection significantly increased. However, we may still find weaknesses and irregularities at some data controllers and processors in certain areas.

The persons liable must eliminate all irregularities and shortcomings, found in inspection procedures. It is worth noting that, as a rule, persons liable do so quickly and on a voluntary basis after receiving a warning by the State supervisor. Unfortunately, however, there are still big problems with persons liable who do not really have business premises but operate only "through" a mailbox and persons liable that registered a foreign national as the responsible person in the Business Register. These are mainly companies that engage in online sales and collect personal data for intrusive direct marketing. The current situation allows the persons liable to perform their activities unlawfully and to avoid liability for violations. Upon the Commissioner's initiative, this issue was addressed by the Inspection Council, which will prepare a proposal of solutions for the competent ministries, the Ministry of Economic Development and Technology and the Ministry of Justice, based on the suggestions, received by the inspection authorities.

The Commissioner observed a large increase in the volume of personal data processed and the widespread nature of such processing in the area of smartphones which are obviously becoming a single point of identification of an individual, a device that enables entry into different systems and services, and a replacement for other devices. With regard to smart devices, the European General Data Protection Regulation recognizes the importance of various online identifiers, the risks of increasing profiling and of automated decision-making. The Regulation will impose on the controllers several requirements for preventive actions; for example, it includes certification mechanisms, a requirement to appointment a data protection officer, conduct impact assessments, respect the principles of privacy by design and by default and the principle of accountability. We estimate that when addressing the issue of data protection, preventive and proactive approaches should be advanced. In any case, this means a major shift in mentality for the data controllers.

The trends that we identified in previous reports continue in the year 2016. Namely, the Commissioner observes an accelerated digitisation of all areas of life with the so-called big data and profiling and the development of artificial intelligence and the Internet of Things. Equally important are areas of genetic and biometric data, where the General Data Protection Regulation leaves the EU Member States more options for maintaining or establishing their rules. The Internet of Things carries challenges especially from the security point of view. Many developers do not see the importance of protecting the new connected points, but they just connect more and more things to the Internet, whether this makes sense or not; for example they connect smart bulbs, refrigerators, sports watches, and increasingly in the recent period, cars. According to some estimates, by the year 2020 there will be up to 30 billion devices connected to the Internet, despite the fact that we deal with privacy issues already with the existing devices. Namely, even the largest data controllers manage systems that are vulnerable, are victims of intrusion into their servers and face data loss.

We must take account of the fact that changes in the field of privacy are rapid. There are less and less areas of life where no personal data are collected, but we hardly even notice this in our everyday lives. Collected data bring power to make decisions, and this power is increasingly transferred from us to someone else; to merchants, operators, the State, intelligence agencies, law enforcement agencies.

Therefore, the Information Commissioner paid special attention to the preventive aspects of its operations in 2016. With the aim of educating data controllers and other persons liable, the Commissioner carried out 96 lectures for domestic audiences free of charge. Taking into account the lectures given to foreign audiences, the number rose to more than 100 lectures carried out free of charge. We are in constant contact with data controllers, processors and proposers of the law in order to give timely advice on different dilemmas regarding new ways of collecting and processing personal data and regarding privacy-friendly statutory solutions while introducing new technologies and increasing efficiency. Among other things, the Commissioner conducted lectures for experts at all the existing ministries who prepare laws and regulations that touch upon the field of personal data protection. The Commissioner also provided more than 120 opinions on laws and regulations that refer to various aspects of managing the collection and processing of personal data.

The Information Commissioner also assists in informal ways with performing data protection impact assessments as one of the basic preventive tools in order to ensure the protection of personal data at an early stage. In 2016, over 100 public and private controllers and processors, who were drafting the legislation, solutions or projects, contacted the Commissioner in order to consult with us in a timely manner on the risks for data protection in order to avoid violations. We also issued four new guidelines and one set of instructions for operators of unmanned aircrafts regarding the performance of data protection impact assessments.

In 2016, the Information Commissioner strengthened the cooperation with stakeholders with the aim of achieving greater synergy and multiplicative effects. With regard to raising awareness of the safe use of the Internet the Commissioner is active in the Safe.si project, cooperates with the Institute for Corporate Security Studies (ICS) and the Agency for Communication Networks and Services. In 2016, the Commissioner signed a cooperation agreement with SI-CERT, a national response centre for dealing with incidents in the field of security of electronic networks and information, and initiated talks on concluding agreements for cooperation with the Association of Banks of Slovenia and the Consumer Association of Slovenia. We are also working closely with the Public Agency for Civil Aviation in educating the operators of unmanned aircrafts.

In 2016, the Commissioner redesigned its website in order to communicate more effectively with its different audiences. Furthermore, as a way of enacting its preventive mission, the Commissioner also cooperated in inter-service working groups and gave talks at various conferences, expert events, consultations and round tables, such as INFOSEK 2016, Cryptoparty 2016, CSA CEE Cloud Security Summit, the Moscow International Conference on Data Protection, 24th International Conference on Auditing, 7th International Conference Corporate Security Days, the Security of Mobile Phones, XV. Labour Law and Social Security Days, the roundtable on The Right to Privacy and New Technologies, the Criminal Law Days, the consultation Digital Conversion Opportunity for Slovenia, the Open Data Festival ...

All of the above signals that the Commissioner will continue to face responsible tasks in the year ahead. A priority task will be to prepare effectively for the implementation of the General Data Protection Regulation. We are pleased to note that many large controllers have already started with the preparation for the use of the Regulation. This is because certain adjustment activities need to be started early enough; the companies need to adjust their business processes, engage suitable staff and assess the existing levels of personal data protection. The task of the legislator is to regulate properly the areas where the Regulation allows the Member States a bit more freedom (e.g. in setting the rules on health, biometric and genetic data). The trend of expending competences of the Commissioner will continue with the adoption of the European e-Privacy Regulation for the single digital market in 2017, which will follow the adoption of the General Data Protection Regulation. In addition, the very nature of modern technologies and the requirements of the society contribute to the constant expansion of the competences of the Information Commissioner as the guardian of privacy and transparency. All this brings us great responsibility, so we will do our best to effectively use our human and financial resources and work towards ensuring the highest possible levels of protection of the two constitutional rights for the residents of the Republic of Slovenia.

Mojca Prelesnik,
Information Commissioner

THE INFORMATION COMISSIONER

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 (hereinafter ZInfP),[1] which established an autonomous and independent State body on 31 December 2005. The mentioned Act merged two previously separate bodies, namely the Commissioner for Access to Public Information, which already had a status of an independent body, and the Inspectorate for the Protection of Personal Data, which was a body within the Ministry of Justice. 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.

This system, comparable to the system of some developed European countries, harmonized the practice of both bodies and helped raising awareness of both the right to privacy and the right to know. These two rights are, thanks to this system, in an even greater harmony than before.

The Information Commissioner is an independent State body. Its independence is guaranteed in two ways. The first guarantee of independence is the process of appointment of the Commissioner as an official by the National Assembly of the Republic of Slovenia upon the proposal of the President of the Republic of Slovenia. The second guarantee is the guarantee of financial independence, namely that the Commissioner is financed from the State budget and the funding is provided by the National Assembly upon the proposal of the Information Commissioner.

From 17 July 2014, the Information Commissioner is led by Mojca Prelesnik.

1.2 Responsibilities of the Information Commissioner

1.2 Responsibilities 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 the field of access to public information, the Information Commissioner is an appellate body, tasked with deciding on appeals against the decisions by which the first instance body refused or dismissed the applicant's request for access, or violated the right to access or re-use of public information. In the context of appeal procedure, the Information Commissioner is also responsible for supervising the implementation of the act that governs access to public information and for supervising the acts adopted thereunder (the competence provided by Article 2 of the ZInfP).

In the field of access to public information, the Information Commissioner also has the competences laid down in Article 45 of the Media Act[2] (ZMed). According to ZMed, the refusal by the bodies liable under this Act to a question posed by a representative of the media shall be deemed a rejection decision. The silence of the body liable is a minor offense and at the same time may be a reason for the appeal. The Information Commissioner decides on the appeal against the rejection decision in accordance with the provisions of the Access to Public Information Act (ZDIJZ).[3]

[1] Official Gazette of the Republic of Slovenia, no. 113/2005 and 51/2007 - ZUstS-A; hereinafter ZInfP.
[2] Official Gazette of the Republic of Slovenia, no. 110/2006 - official consolidated text 1, with amendments; hereinafter ZMed.
[3] Official Gazette of the Republic of Slovenia, no. 51/2006 - official consolidated text 2, with amendments; hereinafter ZDIJZ.

In the field of personal data protection, the Information Commissioner has competences laid down by the Personal Data Protection Act[4] (hereinafter ZVOP-1) and Article 2 of the ZInfP, as follows:

1. Performing inspections over the implementation of the provisions of the ZVOP-1 and other rules governing the protection or processing of personal data, i.e. examines applications, complaints, notifications and other applications where a suspicion of violation is raised, and performs preventive inspections with data controllers in the public and private sector (the competence provided by Article 2 of the ZInfP);
2. Deciding on individual's complaint when the data controller refuses his request for data, extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the act governing personal data protection (the competence provided by Article 2 of the ZInfP);
3. Conducting minor offence proceedings in the field of personal data protection (expedient procedure);
4. Managing and maintaining a register of filing systems, ensuring it is kept up-to-date and publicly accessible through the Internet (Article 28 of the ZVOP-1);
5. Enabling consultation and transcription of data from the register of personal data collections, as a rule on the same day, and at the latest within eight days (Article 29 of the ZVOP-1);
6. Deciding on individual's objection regarding the processing of personal data based on Article 9, Paragraph 4 and Article 10, Paragraph 3 of the ZVOP-1 (Article 32 of the ZVOP-1);
7. Issuing decisions on ensuring an adequate level of protection of personal data in third countries (Article 63 of the ZVOP-1);
8. Conducting procedures to determine an adequate level of protection of personal data in third countries based on the findings from inspections and other information gathered (Article 64 of the ZVOP-1);
9. Maintaining a list of third countries for which it has found that they have fully or partly ensured an adequate level of protection of personal data, or have not ensured such protection. If it has been determined that a third country only partly ensures an adequate level of protection of personal data, the list shall also set out in which part an adequate level has been ensured (Article 66 of the ZVOP-1);
10. Conducting administrative procedures to issue permissions to transfer personal data to a third country (Article 70 of the ZVOP-1);
11. Conducting administrative procedures to issue permissions for connecting official records and public books when at least one filing system to be connected contains sensitive data or if implementation of the connecting requires the use of the same connecting code, such as the personal identification number or tax number (Article 84 of the ZVOP-1);
12. Conducting administrative procedures to issue declaratory decisions on whether the intended introduction of biometric measures in the private sector is in accordance with the provisions of the ZVOP-1 (Article 80 of the ZVOP-1);
13. Cooperating with state bodies, competent EU bodies for the protection of individuals with regard to the processing of personal data, international organizations, foreign supervisory bodies for the protection of personal data, institutes, societies and other bodies and organizations on all issues relevant to the protection of personal data;
14. Issuing and publishing prior opinions to state authorities and holders of public powers regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations regulating personal data.
15. Issuing and publishing non-binding opinions on the compliance of codes of professional ethics, general terms of business or drafts thereof with regulations in the field of personal data protection;
16. Preparing, issuing and publishing non-binding instructions and recommendations regarding personal data protection in individual fields;
17. Publishing on its website or in another appropriate manner prior opinions on the compliance with draft statutes and other regulations with the statutes and other regulations regulating personal data protection as well as publication of requests for constitutional review of regulations, publishing decisions and rulings of courts in relation to personal data protection, as well as non-binding opinions, clarifications, views and recommendations with regard to personal data protection in individual fields (Article 49 of the ZVOP-1);
18. Issuing press releases on performed inspections and preparing annual reports on its work for the previous year;
19. Participating in working groups for the protection of personal data created within the framework of the EU that bring together independent bodies for the protection of personal data in Member States (in the Article 29 Working Party, established under Directive 95/46/EC and in supervisory bodies dealing with processing of personal data in the Schengen Information System and Customs Information System, within the framework of Europol, and in the Eurodac Supervision Coordination Group).

[4]Official Gazette of the Republic of Slovenia, no. 94/2007 - official consolidated text 1; hereinafter ZVOP-1.

The Information Commissioner is also a minor offence body competent for overseeing the implementation of the ZInfP, ZDIJZ in the context of the appeal procedure, and the provisions of the ZVOP-1.

In accordance with Point 6, Paragraph 1 of Article 23a, of the Constitutional Court Act,[5] the Information Commissioner may initiate the procedure for a review of constitutionality or legality of regulations or general acts issued for the exercise of public authority if the question of constitutionality or legality arises in connection with the Commissioner's procedure.

With the entry of the Republic of Slovenia into the Schengen area, the Information Commissioner assumed supervision over the implementation of Article 128 of the Convention implementing the Schengen Agreement and is thus an independent supervisory authority responsible for supervising the transfer of personal data for the purposes of this Convention.

The Information Commissioner also has the competence under:

- the Patient Rights Act[6] (deciding upon complaints by patients and other eligible persons in regard to violation of the right to access medical records, even after the patient's death),
- the Travel Documents Act[7] and the Identity Card Act[8] (supervising the provisions on copying of travel documents or identity cards by data controllers and on storing the copies),
- Electronic Communications Act[9] (exercising supervision over the provisions on disclosure of traffic and location data in cases of protection of an individual's life and body; the provision on tracing of malicious or nuisance calls and disclosure of identification of the calling subscriber; storing data or gaining access to data stored in the terminal equipment of the subscriber or user using cookies and similar technologies),
- Central Credit Register Act[10] (inspection supervision over the collection and processing of personal data in the central credit register and the information exchange system; public disclosure of information related to control measures and sanctions for offenses),
- Consumer Credit Act[11] (supervision of creditors with regard to obtaining data on consumers' creditworthiness and indebtedness).

[5]Official Gazette of the Republic of Slovenia, no. 64/2007 - official consolidated texts 1 and 109/2012.
[6]Official Gazette of the Republic of Slovenia, no. 15/2008; hereinafter ZPacP.
[7]Official Gazette of the Republic of Slovenia, no. 29/2011 - official consolidated text 4; hereinafter ZPLD-1.
[8]Official Gazette of the Republic of Slovenia, no. 35/2011; hereinafter referred to as ZOIzk-1.
[9]Official Gazette of the Republic of Slovenia, no. 109/2012, as amended; hereinafter ZEKom-1.
[10]Official Gazette of the Republic of Slovenia, no. 77/2016; hereinafter ZCKR.
[11]Official Gazette of the Republic of Slovenia, no. 77/2016, as amended; hereinafter ZPotK-2.

1.3 Organization and financial resources of the Information Commissioner

The Information Commissioner carries out its tasks through the following organizational units:

- The Secretariat of the Information Commissioner;
- The Department for access to public information;
- The Department for personal data protection;
- Administrative and Technical Services.

On 31 December 2016, the Information Commissioner had 33 employees, 32 of which on a permanent basis and one temporary employee as a replacement. Compared to 2015, the total number of employees decreased by three persons, while at the same time the number of permanent staff increased by one person.

In accordance with Article 5 of the ZInfP, the Information Commissioner is funded from the State budget and determined by the National Assembly of the Republic of Slovenia upon the proposal of the Information Commissioner. In the beginning of 2016, the budget was set at EUR 1.335.457,02, of which EUR 1.204.845,68 were spent for wages and salaries and EUR 122.008,95 for material costs (e.g. office supplies, printing, cleaning of business premises, monitoring of media reports and archiving (clipping), energy costs, water, utilities, postal services and communication, transport costs and maintenance of official vehicles, travel expenses, professional training expenses for employees) and EUR 5.047,33 for investment (e.g. purchase of office equipment, hardware and telecommunications equipment).

Due to the budgetary constraints and austerity measures adopted by the Government of the Republic of Slovenia in 2016, the Information Commissioner limited the costs for staff trainings and for the scope of its participation in international meetings, and carefully and very restrictively used financial resources on material costs, investment and wages. In addition, the Information Commissioner significantly reduced the costs for publications, student work and other services.

2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

2.1 Legal regulation in the field of access to public information in the Republic of Slovenia

The legislator first guaranteed the right of access to public information in the Constitution of the Republic of Slovenia.[12] The Paragraph 2 of Article 39 stipulates that everyone has the right to obtain public information in which he has a well-founded legal interest under law, except in cases provided for by law. Despite the fact that the right to access to public information is a fundamental human right and as such protected by the Constitution, it was the Public Information Act[13] adopted 11 years later that implemented the right of access to public information. Before that, only individual provisions regarding the publicity of information appeared in some laws, but the ZDIJZ then adopted an integrated approach. This law was adopted by the National Assembly of the Republic of Slovenia at the end of February 2003 and entered into force on 22 March 2003.

ZDIJZ follows the guidelines of international acts and the EU. Its purpose is to ensure publicity and openness of public administration, and to allow everyone access to public information, that is, those related to the working areas of public administration bodies. The Act governed the procedure which ensures everyone free access to and re-use of public information held by State bodies, local government bodies, public agencies, public funds and other entities of public law, public powers holders and public service contractors. It implemented the following Directives of the European Community into the legal system of the Republic of Slovenia: Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, and Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.

In 2005, further steps have been made with the Amendment ZDIJZ-A. Namely, the Amendment narrowed down the possibilities of bodies to hide away public information and introduced many novelties, such as the re-use of public information and the competencies of the Administrative Inspection in the area of implementation of this law. The most important novelty was certainly the public interest test. The law was further improved with the provisions on greater openness in relation to the use of public funds and the information related to the execution of public functions or employment relationship of the civil servant. With this, Slovenia joined the democratic countries that treat exceptions to the openness restrictively, whenever the public interest is at stake.

In 2014, two amendments to ZDIJZ were adopted; ZDIJZ-C[14] and ZDIJZ-D[15]. The most important change that they brought was that the scope of right of access to public information has been duly extended to include companies and other legal entities of private law subject to dominant influence (or majority ownership) of the State, local communities and other entities of public law. In addition, the Agency of the Republic of Slovenia for Public Legal Records and Related Services (hereinafter AJPES) is obliged to establish an online, free-of-charge public Register of legal persons liable for public information within six months after the entry into force of the ZDIJZ-C. The aim of the amendments to the ZDIJZ was to strengthen transparency and responsible management of public funds and financial resources of business entities subject to dominant influence of public entities. The scope of the public control, limited to State authorities, municipalities and the wider public sector, is too limiting. The financial and economic crisis of the past years increased public sensitivity to corruption, abuse of power and poor governance. ZDIJZ-C will also contribute to greater transparency with its provision demanding proactive publication of public information on the websites.

[12]Official Gazette of the Republic of Slovenia, no. 33/1991, as amended; hereinafter: the Constitution.
[13]Official Gazette of the Republic of Slovenia, no. 24/2003, with amendments; hereinafter ZDIJZ.
[14]Official Gazette of the Republic of Slovenia, no. 23/2014.
[15]Official Gazette of the Republic of Slovenia, no. 50/2014 in 19/2015.

The Amendment ZDIJZ-E,[16] adopted at the end of 2015, entered into force on 8 May 2016. It introduced novelties in the field of re-use of public information (e.g. the re-use of information held by museums and libraries, re-use of archives, providing open data for the re-use). The Amendment provides the obligation of authorities to publish on the national Open Data Portal, managed by the Ministry of Public Administration, a list of all databases within their competences together metadata and a collection of open data or a link to websites where open data collections are published. Anyone may re-use data, published on this portal, free of charge for commercial or other purposes, provided that the re-use is carried out in accordance with the ZVOP-1 and that the source of the data is indicated. The Amendment also changes the scope of charging for access and re-use of public information. Only material costs may be charged for access to public information, and not the hourly rates of civil servants who handled such requests. On the basis of the ZDIJZ-E Amendment, the Government of the Republic of Slovenia adopted a new Decree on the provision and re-use of public information,[17] assuming a uniform bill of costs for charging the costs of public information disclosure. It thus eliminated all individual bills, adopted by individual bodies that provided basis for charging of labour costs, and it established the types of public information that should be published on the Internet.

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. 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. For each of the two groups of bodies liable, the term "public information" (i.e. information that they are required to provide to the applicant) is defined differently; it is narrower for the second group of bodies. The definition of information for bodies in general includes all documents, cases, dossiers, registers, records or other documentary material (regardless of whether they have been drawn up by the body, by the body in cooperation with other body, or acquired from other persons). On the other hand, the definition of public information with regard to business entities subject to dominant influence is, in principle, quite the opposite: only those documents, cases, dossiers, registers, records or other documentary material that are so defined by the ZDIJZ are considered public information (e.g. information, related to concluded legal transactions, and information on members of the management, administration and supervision body). For these entities liable, the obligation to provide information is also time-limited, as it only applies to the obligation to provide information, created in the period under the dominant influence. Those bodies liable that meet the criteria for being placed in both groups (for example, companies with a 100% ownership of the municipality, which are at the same time also public service providers) are obliged to provide both types of public information. The entities subject to dominant influence of public entities that are not public bodies may use the so-called simplified procedure for deciding upon the requests (e.g. they do not issue a formal rejection decision, but they only inform the applicant in writing of the reasons why they will not provide the information). Other bodies liable (e.g. the public powers holders, which are at the same time under the dominant influence of public entities) are required to conduct an administrative procedure as specified for the public bodies.

Anyone has the right to access public information, so there is no need to demonstrate legal interest in obtaining it; being curious and having a thirst for knowledge and information is enough. Every applicant has the right to access information upon request by way of consulting the information on the spot, receiving a transcript, a copy or an electronic record. The body liable shall decide upon the request within 20 working days and may, in exceptional circumstances, extend the time limit for a maximum of 30 working days. Consultation on the spot is free of charge. For obtaining a transcript, a copy or an electronic record of the requested information, the body liable may charge material costs. If the body liable does not provide the requested information to the applicant, the applicant has, within 15 days, the right of appeal against the decision or notice by which the body refused the request. The Information Commissioner decides on the appeal. The applicant also has the right to appeal if the body has not responded to the request (the so-called administrative silence) or if the applicant has not received the information in the requested form.

[16]Official Gazette of the Republic of Slovenia, no. 102/2015.
[17]Official Gazette of the Republic of Slovenia, no. 24/2016.

The body may refuse access to the requested information if the request relates to one of the exceptions specified in Paragraph 1 of Article 6 and in Article 5.a of the ZDIJZ (classified information, business secret, personal data, tax secret, court procedure, administrative procedure, statistical confidentiality, document in the making, internal functioning of the body, protection of the natural or cultural value etc.). Without prejudice to these exceptions, access to the requested information is allowed, if the information requested relates to the use of public funds or the execution of public functions or employment relationship of the civil servant. The entity under dominant influence of the State shall not refuse access to absolutely public information (basic information on transactions, regarding expenditure). The business entity can avoid the disclosure of such information only if it proves that this would seriously damage its competitive situation on the market.

If the requested document contains only a part of the information referred to in Article 5.a or Article 6 of the ZDIJZ, this cannot be the reason for the body liable to refuse access to the entire document. If this information can be excluded from the document without jeopardizing their confidentiality, such information is excluded from the document and the rest of the document is disclosed to the applicant. In accordance with Article 19 of the Decree on the provision and re-use of public information,[18] the body must exclude the protected information and allow the applicant access to the rest of the document (consultation, photocopy or electronic record).

The procedure pursuant to Article 45 of the ZMed upon the applicant's request is somewhat different. This is due to the fact that the definition of information according to the ZMed is not identical to public information as defined by the ZDIJZ. Information for the media is a wider term, because it also includes preparation of answers to the questions (e.g. explanations, interpretations, analyses and comments). If the media requests that a body answers its question, such application will be dealt with in accordance with provisions of the ZMed. On the other hand, if the media requires access to a document, such application will be dealt with in accordance with the ZDIJZ. The media should submit the question in writing by regular or electronic mail (no digital certificate or electronic signature is required) and the body must notify the media in writing that it intends to refuse or partially refuse to answer the question by the end of the next business day. Otherwise, the body must submit to the media the answer to the question no later than within seven working days after receiving the question, whereas the answer may only be refused if the requested information is exempted from free access in accordance with the ZDIJZ. After receiving the answer, the media may demand additional explanations which the body must provide to him no later than within three days. If the body does not hold the information which gives the answer to the question in a materialized form, the media cannot appeal against the refusal or partial refusal. The appeal is permitted only when the answer to the question derives from a document.

[18]Official Gazette of the Republic of Slovenia, no. 76/2005, 119/2007 and 95/2011.

2.2 Number of appeals lodged and number of cases resolved

In 2016, the Information Commissioner received 514 appeals, of which 316 were against the refusal decisions and 198 were against the non-responsiveness of the first instance bodies (the so-called administrative silence).

In appeal proceedings against decisions in which the bodies liable refused requests for access to or re-use of public information, the Information Commissioner conducted 22 procedures against the business entities under the dominant influence of the State, self-governing local communities and other public entities. The Commissioner issued 312 decisions and in two cases it dismissed the appeals on procedural grounds. In the course of handling the appeals, the Commissioner conducted 76 in camera inspections, which are inspections without the presence of the parties requesting the documents in order to establish the facts of the case, namely the existence of the documents at the body liable.

In proceedings against the administrative silence, the Information Commissioner first called on the bodies liable to decide on the applicant's request as soon as possible. In the majority of cases, upon receiving summons of the Information Commissioner, the bodies liable decided on the request of the applicant and provided the requested information to the applicants. After the body liable had responded, the proceedings against the administrative silence were completed, and the applicants who received the refusal decision had the opportunity to appeal to the Information Commissioner against such a decision. In 26 cases, the Information Commissioner dismissed the appeal on procedural grounds with a decision (15 of these applications were premature and 11 incomplete). Six individuals withdrew their appeals because they received the requested information, and in six cases the Information Commissioner advised the applicants that it was not competent to consider their applications and transferred their cases to competent authorities for consideration.

In 2016, the Information Commissioner received 308 requests for assistance and various questions from individuals regarding access to public information. The Information Commissioner replied to all the applicants within the framework of its competences, in most instances it referred the applicants to a competent institution. Namely, the Information Commissioner is a second instance body that decides on the appeals and it is not competent to answer specific questions on whether information should be deemed public or not, especially at the stage when the first instance body has to decide on this question. In accordance with Article 32 of the ZDIJZ, the ministry responsible for public administration provides opinions on access to public information.

2.3 Number of filed actions at the Administrative Court of the Republic of Slovenia, number of judgments of the Administrative and Supreme Court of the Republic of Slovenia

An appeal against the decision of the Information Commissioner is not allowed, but it is possible to initiate an administrative dispute. In 2016, 43 administrative disputes were issued against decisions of the Information Commissioner, i.e. against 12.9% of all decisions issued. The share is relatively small, which indicates a great level of transparency and openness in the operations of the public sector, as well as the acceptance of the Commissioner's decisions by the bodies liable and the applicants.

In 2016, the Administrative Court issued 22 judgements regarding decisions of the Information Commissioner in which it decided to:
- Dismiss the application as unfounded – 8 cases;
- Uphold the application, annul the decision in part or in its entirety and refer the matter to the Information Commissioner for reconsideration – 6 cases;
- Dismiss the application on procedural grounds in one part, but in the other part uphold it and annul the decision of the Information Commissioner and refer the matter to it for reconsideration – 4 cases;
- Dismiss the application on procedural grounds – 2 cases;
- Uphold the application, so that it annulled the Commissioner's decision in one part and dismissed the application in the other part – 1 case;
- Dismiss the application in one part and stopped the procedure in the other part – 1 case.

In 2016, while the Information Commissioner did not file any requests for revision against the ruling of the Administrative Court, five bodies liable did so. By the end of 2016, the Commissioner did not receive any decisions of the Supreme Court.

2.4 Statistics by individual fields of the ZDIJZ

Compared to previous years, in 2016 the number of decisions issued in the field of access to public information slightly increased. The Information Commissioner issued 312 decisions, which is the highest number so far.

The Information Commissioner issued the following decisions:
- In 141 cases it granted the appeal partially or entirely in favour of the applicant;
- In 137 cases it refused the appeal;
- In 29 cases it granted the appeal and returned the matter to the first-instance body for reconsideration;
- In 3 cases the first instance decision was declared null;
- In 2 cases it dismissed the appeal on procedural grounds.

In its decisions the Information Commissioner made substantive rulings with consideration of the following:
- Whether the body possessed the document or the public information requested by the applicant – 104;
- Whether the documents requested contained personal data disclosure of which would result in a violation of personal data protection in accordance with the ZVOP-1 – 84;
- Whether the applicant requested information or data deemed to be a business secret in accordance with the law governing companies – 55;
- Whether a violation of procedural rules occurred – 46;
- Whether the public interest in disclosure outweighs the public interest or the interest of other persons in restricting access to the information requested – 27;
- Whether the information requested pertains to the document drawn up in connection with internal operations or activities of bodies, and the disclosure of which would cause disturbances in operations or activities of the body – 25;
- Whether the information requested relates to the work and personal data of civil servants and officials – 23;
- Whether the information originates from the field of work of the body – 20;
- Whether the requested information is protected by copyright legislation – 16;
- Whether the case concerns environmental information – 16;
- Whether the decision was issued after the Administrative Court's judgment – 14;

- Whether the information requested pertains to data obtained, compiled for or relating to a criminal prosecution or minor offence proceeding, whose disclosure would be harmful to the implementation of such proceedings – 14;
- Whether the applicant abused his/her rights under the ZDIJZ – 13;
- Whether the information requested pertains to data classified in accordance with legislation regulating classified information – 13;
- Whether the document requested meets the conditions for it to be deemed public information as provided for in Paragraph 1 of Article 4 of the ZDIJZ – 13;
- Issuing the decision in procedures in which the applicant requested documents related to public procurement procedures – 12;
- Whether the body to whom the request for access to public information was addressed to is in fact liable under Paragraph 1 of Article 1 of the ZDIJZ – 8;
- Whether the information requested pertains to data in the document that is in the process of being drawn up and is still subject of consultation by the body, and the disclosure of which would lead to misunderstanding of its contents – 7;
- Whether the requested information pertains to data that was acquired or drawn up for the purposes of administrative procedure, and the disclosure of which would prejudice the implementation of such procedure – 6;
- Whether the information requested pertains to data that was acquired or drawn up for the purposes of civil, non-litigious civil procedure or other court proceedings, and the disclosure of which would prejudice the implementation of such procedures – 4;
- Whether the body violated a substantive law – 4;
- When the body did not issue a decision to the applicant in relation to the requested documents, but provided him with public information that he did not even request – 4;
- Whether the information relates to the issue of confidentiality of a source – 4;
- Whether the case concerns the re-use of public information – 4;
- Whether the authority correctly charged the fees for providing public information – 4;
- Whether the requested information pertains to data whose disclosure would constitute an infringement of the tax procedure confidentiality or of tax secret in accordance with the act governing tax procedure – 3;
- Whether the requested information pertains to data, access to which is forbidden or restricted under law even to parties, participants or victims in legal or administrative proceedings, or inspection procedure as governed by the law – 2;
- Whether the information is marked with a level of secrecy contrary to the law governing classified information - 2,
- Whether the body referred the case to another body which is competent to handle it based on its contents – 2;
- Whether the case concerns the proactive publication of information – 1;
- Whether the requested information pertains to data disclosure of which would constitute an infringement of the confidentiality of individual information on reporting units, in accordance with the act governing Government statistics activities – 1.

The Information Commissioner‘s decisions in appeal proceedings against refusal decision concerned the following groups of bodies:
- State authorities (128 cases), from which ministries, constituent bodies and administrative units (106 cases), and courts, Supreme State Prosecutor and State Attorney‘s Office (22 cases),
- Public funds, public institutes, agencies, public service contractors, bodies exercising public powers and other public entities (115 cases),
- Local government authorities (47 cases),
- Business entities subject to dominant influence of public entities (22 cases)

172 appeals were submitted by natural persons, 98 by private sector legal entities, 38 by journalists, and four by public entities.

2.5 Minor offenses proceedings for the violation to ZDIJZ, ZInfP and ZMed

In 2016, the Information Commissioner initiated two minor offences proceedings, namely:

- One for a minor offence under Paragraph 2 of Article 39 of the ZDIJZ as the body destroyed the requested public information;
- One for a minor offence under Article 15 of the ZInfP, as the body failed to provide public information despite the Commissioner's decision ordering it to do so.

In both cases, the Commissioner issued a warning to the offenders.

2.6 Most significant decisions of the Information Commissioner in different areas

We present some of the most complex and interesting decisions from 2016, sorted by areas.

2.6.1 Environmental information; protection of the administrative procedure

By decision No. 090-38/2016/10 of 5 May 2016, the Information Commissioner instructed the Ministry of Infrastructure (the body) to allow the applicant access of a draft Renewable Energy Sources Action Plan (ANOVE).

The body rejected the applicant's request in full, referring to the exception from Point 7 (the protection of the administrative procedure) and Point 9 (document being drawn up), Paragraph 1 of Article 6 of the ZDIJZ. The body explained that the requested document is a part of an administrative procedure relating to the comprehensive environmental impact assessment conducted by the Ministry of the Environment and Spatial Planning. There are several bodies involved in this process, as well as a large number of documents. The body believes that allowing the applicant access to the requested document would lead to delays and disruptions in the administrative procedure. Early disclosure of the document during the consultation and reconciliation process would also lead to a misunderstanding of its contents.

In the appeal procedure, the Information Commissioner did not confirm the explanation of the body, as it assessed that the disclosure of information would not prejudice the implementation of the administrative procedure. Namely, the body did not prove that allowing access to the document would lead to delays and interruptions in the procedure, but it merely anticipated that there would be possible delays. The possibility of such abstract delays in the procedure (which, according to the body, lasts from 2014, while the applicant made his request in 2016), does not pose a real threat to the process.

In addition, the Information Commissioner did not agree with the body's standpoint that the document at hand is still in the process of being drawn up. Namely, this exception cannot be used in procedures with multiple phases where different versions of the same document are being produced. A mere fact that the document represents one of the completed versions of a document does not mean that it is still in the process of being drawn up and still subject of consultation. Each completed version of the proposed document represents an independent public information.

The Information Commissioner also noted that the requested document contains environmental information, and such information is absolutely public on the basis of Point 2, Paragraph 3 of Article 6 of the ZDIJZ. The Information Commissioner further explained that procedures, closed and non-transparent procedures do not have a positive influence on the confidence of the public, which is essential in such important cases that concern the environmental protection. Only if the State bestows confidence in the critical assessment of the public, it is possible to create an impression in the public that the State's actions are trustworthy and that the procedures for environmental protection are being conducted in the public interest.

2.6.2 Media; civil servants; the body's field of work

By decision No. 090-263/2015/7 of 7 January 2016, the Information Commissioner ordered the Faculty of Economics in Ljubljana (the body) to provide the applicant with a list of 149 copyright and work contracts concluded with Dušan Mramor from 1 January 2005 to 17 September 2015, and with the copyright contract for a scientific monograph.

As a journalist, the applicant requested answers to questions, which the body rejected this and stated that it cannot disclose the contents of the copyright and work contracts to her, as this would mean the disclosure of protected personal data. The copyright and work contracts are not related to the performance of a public function or the employment relationship of a civil servant, and consequently there is no use of public funds involved. At the in camera inspection it was also discovered that the contracts were concluded with Dušan Mramor only in his capacity as a natural person.

In the appeal procedure, the Information Commissioner did not follow the explanation of the body. The Commissioner reviewed the contracts and concluded that they refer to the fields of work that relate to the exercise of the public service of the body. Namely, they were contracts for the implementation of activities that are defined as lectures in part-time studies, seminars and courses, preparation of textbooks and study materials, preparation of study programmes, lectures and seminars within the framework of the full-time study programme, exercises, examinations, mentoring, conducting and assessing the exams, etc. The Commissioner explained that these activities are without a doubt a part of exercising the public service. The mere fact that a particular activity of the body is not financed directly from the budget, as claimed by the body, does not take away its status as a public service.

The Information Commissioner also did not follow the body's explanation regarding the exception of personal data protection, referred to in Point 3, Paragraph 1 of Article 6 of the ZDIJZ. This is because such information is related to the use of public funds, which means that personal data of the recipients of fees under copyright and work contracts enjoy a significantly reduced level of protection. At the same time, the Information Commissioner found that the work agreed within the copyright and work contracts falls within the scope of the work obligations from the regular employment relationship of a civil servant. On the basis of Point 1, Paragraph 3 of Article 6, access to information, without prejudice to the exception of the protection of personal data, is permitted in case the information is on the use of public funds or it relates to the performance of a public function or the employment relationship of a civil servant.

The Information Commissioner also carried out a public interest test and decided that the public interest in disclosing the name and surname of the recipient of the fee and the amount of the gross fee is stronger than the individual's interest in not informing the public on such information. In the concrete case, the requested information is necessary in order to ensure greater responsibility in deciding on the use of public funds and the possibility of informed public participation in the public debate on this important topic.

2.6.3 Document in the process of being drawn up

By decision No. 090-23/2016/5 of 23 March 2016, the Information Commissioner ordered Nigrad, d. d. (the body) to provide the applicant with working drafts of the materials for the public presentation of the project for the discharge of wastewater and rainwater.

The body rejected the applicant's request in full, referring to Point 9, Paragraph 1 of Article 6 of the ZDIJZ, namely to the exception of the document being drawn up. The body explained that the applicant's request relates to the materials that are still in the process of being drawn up, and is also the subject of consultation of a joint meeting of representatives of public companies and heads of municipal council groups of the Municipality of Maribor. The disclosure of such information would, according to the body, lead to a misunderstanding of its contents.

The Information Commissioner assessed whether the document fulfils all three conditions for the said exception, and decided that the body did not demonstrate in its decision that the disclosure of the document would cause a misunderstanding of its contents. It is perfectly clear that this is a non-binding working material, and that it contains comments that will be the subject of discussion. This makes it clear to anyone that the matter may be subject to changes and additions, which can occur at any point in time.

The Information Commissioner also noted that the material had already been disclosed to third parties, whereas the body did not prove that the disclosure would cause damage to the body or that there would be any problems with understanding the material.

2.6.4 Business entities under dominant influence

By decision No. 0902-14/2016/4 of 20 December 2017, the Information Commissioner decided that the contract concluded between the UPS, d.o.o., and Pošta Slovenije (the body) does not refer to the provision of universal postal services nor does it fulfil the conditions for public information pursuant to Article 4.a of the ZDIJZ and it thus rejected the appeal. The Commissioner referred the case back to the body of first instance for a new decision regarding the access to contracts with the GLS, d.o.o. and the UPS Adria (s) Ekspres.

In its decision, the body stated that it is liable for providing public information only in the part of its activities in which it is authorised to provide a universal postal service. In the rest of its activities, it is liable as a business entity under the dominant influence. The requested information relates partly to universal postal services, partly to other postal services and partly to commercial services provided by the body. Therefore, this information does not constitute public information in its entirety.

The Information Commissioner followed the explanation of the body in part which relates to access to the contract concluded with UPS, d.o.o. The services performed on the basis of the aforementioned contract do not constitute the universal postal service. Additionally, the content of this contract does not relate to obtaining, using or managing tangible assets of a business entity or expenditures of a business entity on a contract on supply, works, or agent, consulting or other services, as well as sponsor, donor and contractual agreements and other legal transactions of equal effect. Therefore, this contract does not constitute public information.

In the part relating to the contract concluded with GLS and UPS Adria (s) Ekspres, the Information Commissioner found that the body did not fully investigate the facts of the case relating to the issue of universal postal service. In addition, the body did not call third-party participants to join in the procedure. In this part, the Information Commissioner set aside the decision of the body and ordered that in the renewed procedure, the body clearly defines which parts of the contracts relate to providing the universal postal service and consequently which parts of the contracts fall within the body's field of work in terms of performing public-law tasks, referred to in Article 4 of the ZDIJZ.

2.6.5 Business secret; the use of public funds

The Information Commissioner, by decision No. 090-148/2016/5 of 22 July 2016 set aside the refusal response from the Begunje Psychiatric Hospital (body) and instructed the body to provide the journalist the information on manufacturers of medicines and medical devices supplied in 2015 and in the first trimester of 2016 by the company Sanolabor, d.d.

The body provided the requested information to the applicant, but redacted the catalogue numbers and information on manufacturers, stating that this information is considered a business secret.

The Information Commissioner did not follow the position of the body. While Sanolabor, d.d., identified the redacted information in its internal acts as a business secret, the provision of Paragraph 3 of Article 39 of the Companies Act explicitly provides that information that is public by law or information on violations of the law or good business practices cannot be considered as business secret. In this case, the information was on the use of public funds, so the Commissioner allowed access to the requested information in accordance with Point 1, Paragraph 3 of Article 6 of the ZDIJZ.

2.6.6 Environmental data

By decision No. 090-120/2016/10 of 6 September 2016, by which a previous decision was supplemented, the Commissioner rejected the applicant's complaint concerning data on water levels of the River Drava. The reason for the rejection was that the requested document does not exist.

Upon deciding on the applicant's request, the Environmental Agency of the RS (the body) ignored that the applicant was also interested in data on water levels, and not only data on the flows of the River Drava in the hydroelectric power plant area. In the appeal procedure, the Information Commissioner found that the body does not dispose of the information on water levels of the Drava River. The body does not obtain this information from the company DEM, d.o.o., which manages water in the framework of the public utility service, or from any other source. Accordingly, the Information Commissioner concluded that the decision of the body was consistent with the law but was reasoned with incorrect reasons, and therefore rejected the appeal on the basis of Paragraph 3 of Article 248 of the General Administrative Procedure Act.

2.6.7 Classified information

By decision No. 090-160/2016/3 of 27 October 2016, the Information Commissioner ordered the Institute for Commodity Reserves (the body) to withdraw the "internal" level of classification, and to provide the applicant with certain orders and sales contracts.

The body assessed that the disclosure of contracts would reveal the information on the dynamics of the procurement of the safety wire fence and such disclosure would jeopardize the execution of the public procurement, the operation and implementation of certain tasks of the Government of the Republic of Slovenia, and the safety of the supplier's personnel or its collaborators. Consequently, the goals of the Government of the RS for the effective regulation of migrant flows at the State border, necessary for securing the essential security interests of the Republic of Slovenia, its population and assets, would be jeopardized.

The Information Commissioner did not follow the body's reasoning. Despite the fact that the requested documents fulfilled both the material and the formal criteria for classified information, the Commissioner weighed up all the arguments and concluded that access to the contracts should be allowed. Namely, the applicant requested only data from the contracts that were already implemented in full and based on which the successful bidder has already received the payment. The amounts received by the supplier have already been in the public domain and the fact that the wire fence had been purchased and placed on the State border was also already known.

The Information Commissioner decided that it is in the public interest that the public be fully informed of the information on the use of the public funds in connection with the purchase and placement of a border fence. Namely, the damage that would be caused to the body is not greater than the public's interest in being thoroughly acquainted with the requested information. It is in the public's interest in a democratic society to have access to impartial and objective information, on the basis of which the public can make informed

decisions on public law matters and thereby control the use of public funds.

2.6.8 Confidentiality of the source

The applicant requested that the Inspectorate for the Environment and Spatial Planning (the body) grants him access to the copy of an anonymous report on an illegal construction. The body rejected the request referring to the exception of confidentiality of the source of the report under Article 5.a of the ZDIJZ. The body expressed the view that the exception of the confidentiality of the source protects both the applicant and the content of the report.

By decision No. 090-1/2016 of 11 February 2016, the Information Commissioner decided that the body interpreted the protection of the confidentiality of sources, regulated by the Inspection Act (ZIN) in conjunction with Article 5a of the ZDIJZ, too broadly. The Commissioner decided that the confidentiality of the source of the report protects only the applicant's privacy, but not the content of the report itself. In accordance with Paragraph 1 of Article 16 of the ZIN, the inspectors are obliged to protect all types of confidentiality they get acquainted with in the course of their work (for example, business secrets), while Paragraph 2 regulates the confidentiality of the source of the report and of other information. The Information Commissioner took the view that the confidentiality of the source only encompasses the protection of the privacy of the applicant, while the contents of the report can be protected by another category of protected information in accordance with Paragraph 1 of Article 16 of the ZIN (for example, if the report is a business secret). The body also referred to two judgments (namely, the judgments of the Administrative and Supreme Court, No. U 313/2004 and No. X Ips 775/2006). However, as none of these decisions were taken on matters relating to access to public information, they are irrelevant to the case in hand. In accordance with the above, the Information Commissioner upheld the appeal and granted access to the anonymous report.

2.6.9 Media; law enforcement

A journalist requested from the Municipality of Maribor (the body) access to the audit report on the extraordinary audit of operations of the public institution Športni objekti Maribor for the year 2014. The body rejected the request. The District State Prosecutor's office in Maribor was also called upon regarding the requested report. It turned out that the requested report was part of materials, important for the prosecution of a perpetrator, from the pre-trial procedure. Accordingly, the body rejected the request for access pursuant to Point 6, Paragraph 1 of Article 6 of the ZDIJZ.

By decision No. 090-45/2016 of 23 March 2016, the Information Commissioner confirmed the decision of the body of the first instance on the grounds that the exception to the protection of law enforcement under Point 6, Paragraph 1 of Article 6 of the ZDIJZ also includes a pre-trial procedure (namely, all measures for detecting criminal offenses and their perpetrators). According to the explanation of the Prosecutor, the audit report is an integral part of materials in the pre-trial procedure and it should not be disclosed, not even in its individual parts. The Information Commissioner also assessed that the Prosecutor sufficiently explained the damaging effects that the disclosure of the requested audit report would cause. Disclosing the report would prejudice the implementation of a concrete (pre-trial) criminal prosecution and the damage would outweigh the public's right of access to the content of the requested document. The criteria laid down by the ZDIJZ in order to confirm the existence of the exemption under Point 6, Paragraph 1 of Article 6 of the ZDIJZ were met cumulatively. Thus, the Information Commissioner dismissed the appeal of the journalist as unfounded.

2.6.10 Is the body liable?

The journalist of Val 202 Radio requested from the Nuclear Power Plant Krško, d.o.o. (the NPP) access to information about the anticipated price of security upgrades that were foreseen in the National Action Plan after the Fukushima accident, information on how much funds have already been spent on the upgrades, how much will there still need to be paid, and when the upgrades are expected to be realized. The NPP replied, but the applicant appealed against this response, complaining that he did not receive the answer to the question on the planned and realized funds needed for the upgrades.

In the appeal procedure, the Information Commissioner found that the NPP was not registered in the Register of persons liable. The legal status of the NPP changed due to the ratification of the international treaty between the Republic of Slovenia and the Republic of Croatia, which transformed the Krško NPP into a company with

limited liability. Following this change, the Krško NPP is no longer a public law body, and in accordance with its registered activity, it also does not perform public service and is not a holder of public powers. The Information Commissioner found that the Krško NPP does not fall among the bodies liable under Paragraph 1 of Article 1 of the ZDIJZ (i.e. the bodies), neither among the persons liable under Article 1.a of the ZDIJZ as an entity under the dominant influence of public entities. The relationships within the Krško NPP are regulated according to the parity principle, which means that the relationships between the parties to the contract follow the principles of "harmonisation and proportionality". For this reason, it is impossible to conclude that the Krško NPP is under the dominant influence of public entities. The Information Commissioner found that the Republic of Slovenia does not own more than 50% of NPP's share of the business, since the ratified international agreement explicitly agreed that ELES GEN, d.o.o., Ljubljana, has an exact 50% business share, which does not represent a "majority share". In the NPP, the Republic of Slovenia does not have the right to supervise the majority, neither is it entitled to naming more than half of members of the management body or the supervisory authority, as the company bodies are compiled in parity, i.e. precisely half of members of each contracting party. This means that the Republic of Slovenia through ELES GEN, d.o.o., Ljubljana, cannot exercise the dominant influence, as foreseen by regulation encompassed in the ZDIJZ. The Information Commissioner therefore concluded that the Krško NPP is not a body liable for providing public information (decision No. 0902-8/2016 of 9 May 2016).

2.6.11 Internal operation of the body; business secret

The journalist from the Municipality of Maribor (the body) requested access to the agreement between the body and a potential foreign investor for the purchase of municipal real estate. The body rejected the request on the grounds that the disclosure would cause a disturbance in its operation, namely that the potential investor would lose his confidence, which would, the body believes, influence the success of the sale. Since the investor has invested in municipal projects in the past, there was a concern on the part of the body that this would have a negative impact on good business relations (and therefore on future projects). This would also be reflected in the loss of business opportunities and consequently in the loss of profit.

The Information Commissioner found (by decision No. 090-301/2015 of 13 May 2016) that the exception to free access regarding internal operations in accordance with Point 11, Paragraph 1 of Article 6 of the ZDIJZ, alleged by the body, is not proven. Namely, the document does not relate to the internal operations of the body; to the contrary, it explicitly relates to its external operations. The document was concluded abroad as a statement of direct readiness to cooperate with the potential investors. The disclosure could not have any effect on the process of selling municipal real estate, because this process is strictly regulated by public law and the sectoral regulation provides for a heightened transparency. In addition, the requested document is not a type of act that is foreseen in the process of sales. The Information Commissioner also established that the document meets the subjective criterion for the existence of a business secret, as Article 6 of the requested agreement meets the criteria of a "written decision" from Paragraph 1 of Article 39 of the ZGD-1. Nevertheless, the Information Commissioner assessed that certain information in the agreement cannot be determined as a business secret, because certain information relates to the use of public funds and the employment relationship of civil servants or the performance of a public function. This information is public in accordance with the law. The Information Commissioner thus decided that the essential elements of the agreement (the purpose of the agreement and the understandings of the parties) represent information related to the use of public funds. Namely, the requested document included the intention to sell / buy municipal real estate, in which the parties expressed their interest and identified the real estate with plot numbers. In order to ensure that the disposal of public real estate is economical, the management of such property is governed by an emphasised principle of transparency, which enables the public to supervise the operations of the authorities.

2.6.12 Re-use

The Information Commissioner decided in a case of the applicant's appeal against the decision of the Surveying and Mapping Authority of the Republic of Slovenia (the body) on the re-use of public information and against the invoice issued on the basis of this decision. The Information Commissioner found that it was disputed whether the applicant had even submitted a request for re-use and what exactly he requested.

The applicant filed a request with the body on a pre-prepared form that enables access to "online services for the purposes of re-using the public information." On the basis of this request, a contract was signed on 15 December 2015 on the transfer and the use of electronic service for the acquisition of geodetic data (hereinafter referred to as the contract). The conclusion of the contract and the price of the particular online service are governed by the sectoral rules. Later, on 12 April 2016, the body issued a decision on the re-use of information and the invoice for the payment of the price of re-use, which was then challenged by the applicant in the appeal procedure before the Information Commissioner on the basis of the ZDIJZ.

The Information Commissioner found that a written request had never been filed by the applicant, so by issuing a decision without the request, the body committed an infringement of essential procedural requirements. Neither the order of the services provided by the online service provider nor the contract to provide these services may be interpreted as the applicant's request for the body to initiate an administrative procedure for the re-use of public information. With regard to the invoice issued, the Information Commissioner found that the body included in the price of the re-use the costs of providing the online service in accordance with the aforementioned rules, which the ZDIJZ does not provide for.

Consequently, the Information Commissioner referred the case back to the body of the first instance (decision No. 090-105/2016 of 22 June 2016), instructing the body to first clarify the question of what the applicant requested, namely an online service or a re-use of public information. The Commissioner pointed out that the explanations on the body's website regarding the access to the online services for the purposes of re-use of public information are misleading, because a lay person can easily confuse the purposes and the effects of both regimes. The Information Commissioner emphasized in its decision that when a request for the re-use is dealt with in substance, the body should follow the rules in the field of access to public information, and therefore the price of the online service should not be included in the price of the re-use. The Commissioner added that the body should not conclude contractual relations on the rights of the applicant, which are established by the ZDIJZ. Finally, the Information Commissioner stated its position on the importance of the principle of non-discrimination, deriving from Article 36 of the ZDIJZ. In particular, the Commissioner emphasised that when the body uses the information for performing activities that are not part of its official tasks, the body is subject to the same price and other conditions when it wishes to use such information itself. The re-use of information must be permitted and enabled for all applicants or users, at the same price and under the same conditions, even if such a user is the body itself.

2.6.13 Classified information; withdrawal of classification

The applicant requested from the Ministry of the Interior (the body) a report drawn up by the Police and Security Directorate (hereinafter referred to as PSD) concerning the case of information intrusions into computer systems, in which the Slovenian police was allegedly involved. The case launched a wider debate in the media,[20] and it was also discussed by the National Assembly of the Republic of Slovenia.[21] The requested report was marked internally with the classification level "internal", so the body refused access to the document on the basis of the exception of the protection of classified information (Point 1, Paragraph 1 of Article 6 of the ZDIJZ). In the complaint, the applicant relied on the overriding public interest in the disclosure, since the document allegedly revealed serious invasions of individuals' privacy by the Police, and therefore the disclosure of the document is (at least with regard to irregularities in the operation of the Police) in the prevailing public interest.[22]

The Information Commissioner confirmed the body's standing that the requested information was classified (all criteria for classifying the documents were met). At the same time, there is a prevailing public interest in disclosing the introduction and the conclusion part of the requested report, which describe the overall conclusions and foresee measures deriving from the supervision carried out by PSD. In order to substantiate the prevailing public interest, the Information Commissioner took into account that the Police is a repressive authority, which is very clearly tasked with an obligation to protect public security and the respect human

rights and fundamental freedoms. It is therefore in the great interest of the public to be aware of the relevant information regarding the activities of the Police, especially when they point to alleged violations of the human rights. The Commissioner also took into account that a wider public debate took place around this issue, and held that the disclosure of the requested documents could significantly add to the public awareness of the relevant information in this case. Finally, the Information Commissioner took into account the current public discourse regarding the planned changes with regard to expanding police powers; the disclosure of the requested information could give a meaningful contribution to this discourse. Taking into account all of the above, the Information Commissioner decided that the body should remove the classification level "internal" from the introduction and conclusion of the requested document and disclose it to the applicant in this part. The Commissioner concluded that other parts of the document containing information on persons, tactics and methodology of the police work with informants and sources, which would endanger the security of persons and the work of the police if disclosed, have been rightfully classified. In this part, the Information Commissioner therefore assessed (by Decision 090-213/2016 of 10 November 2016) that the State's interest in securing confidentiality of information prevails over the public's interest in disclosure.

[20]See publications: »Police: The statements of Ornig, that the leadership knew about the intrusions, are misleading« (rtvslo.si, 15 June 2016); »The intrusion into electronic communications: The Police wishes to sweep the Oring case under the carpet« (dnevnik.si, 3 June 2016); »Hacking on demand?« (vecer.si, 15 June 2016); »First he found the liability in the Police frequencies, now he's under investigation « (zurnal24.si, 30 April 2016), »The statement of Dejan Ornig, the informant that hacked private communications of individuals for the Police« (podcrto.si, 11 June 2016).

[21]Commission for Supervision of Intelligence and Security Services, 21.st emergency meeting, 17 March 2016.

[22]Without prejudice to the provisions on the exceptions, access to the requested information is sustained, if public interest for disclosure prevails over public interest or interest of other persons not to disclose the requested information, except for information which, pursuant to the Act governing classified data, is denoted with one of the two highest levels of secrecy (Point 1, Paragraph 2 of Article 6 of the ZDIJZ). In the present case, the requested documents were classified with the classification level internal, which is not one of the two highest levels of secrecy. Thus, it was permissible to use the institute of the prevailing public interest for disclosing the document.

2.7 General assessment and recommendations in the field of access to public information

In 2016, the Information Commissioner received 514 complaints in the field of access to public information. It received 316 appeals against rejection decisions and 198 complaints against the administrative silence. The Information Commissioner received 308 requests for an opinion or clarification from the applicants and bodies liable. In total, the Commissioner handled 822 matters.

According to the figures given, the Information Commissioner welcomes the fact that the number of complaints due to the so-called administrative silence has been significantly reduced. Comparing to the previous year, this number fell by 37%, while the number of requests for opinions and clarification increased. This suggests, that in 2016, the bodies liable have been more active and responsive than in 2015, and that they contacted the Information Commissioner more frequently with requests for guidance outside the appeal procedure too.

Compared to the year before, the number of complaints against rejection decisions stayed about the same, while the Commissioner again issued more decisions than ever before in all of the years this institution has been active. The Information Commissioner strived for swift handling of the appeals with a minimum delay for the applicants. The average time to decide upon an appeal against the rejection decision, in which a special declaratory procedure was required, was 47 days, which is less than in the year 2015, when the average time was 62 days. In 2016, the Information Commissioner processed 22 complaints against the decisions of entities under dominant influence, which is more than in the year 2015, when this number was 15. Nevertheless, it is worth noting that the percentage of such complaints in relation to all the complaints is very low (4%). This leads us to a conclusion that the situation has "stabilized" after the entry into force of the Amendment ZDIJZ-C with regard to the new bodies liable. In addition, the statistics on the complaint cases against the business entities under dominant influence demonstrate that these entities do not bear an excessive burden with implementing the ZDIJZ.

The statistics also show that the majority of appeals against rejection decisions were against State authorities (which includes all State bodies, ministries, constituent bodies, administrative units, courts, Supreme State Prosecutor and State Attorney's Office). Namely, there were 128 such appeals in 2016, while there have been 156 in the year before. It should be noted, however, that this is the widest group of bodies liable, which in practice also receive the largest number of requests for access to public information.

As in the previous year, the Commissioner assesses that (even) more efforts are needed for active training of all bodies liable regarding the use of the law in practice. For example, the Commissioner was active in the course of preparations for the use of Amendment ZDIJZ-E in the training sessions for the bodies liable, organised by the Ministry of Public Administration.

In 2016, the Information Commissioner considered several important appeal cases in regards to their substance. An interesting piece of information is worth noting with regard to the exceptions relied upon by the bodies liable. Namely, the largest number of complaints did not concern the exception of personal data protection (as in previous years), but the question whether the requested information even exists. This is probably partly due to the fact that in the times of rapid information technology development, the applicants expect the bodies liable to have at hand various statistical information and the possibility to search for information according to different criteria. In practice, however, it often turns out that the bodies do not hold information for their own organisational needs with such a content or in such a way or form as the applicant requested. The bodies liable are not obliged to analyse data, prepare extracts, summaries, explanations and answers to questions to satisfy the applicant's request under the ZDIJZ. In such cases, the procedure is concluded with the conclusion that the requested information does not exist and, consequently, the Commissioner issues a rejection decision. In majority of cases when the requested information does not exist and the body liable is not obliged to create it, the Information Commissioner rejects the complaint as unfounded. This is also reflected in the overall share of rejected complaints, which rose in 2016 (40% of complaints were rejected in 2015, and 44% in 2016).

The data show that the structure of the applicants who filed complaints remained more or less the same as in the year before. The majority of the complainants were individuals - natural persons (172), followed

by legal entities of private law (98) and journalists and media outlets (38). It is interesting to note that legal entities governed by public law also acted as applicants in the appeal proceedings before the Information Commissioner (4).

In 2016, as in the year before, the Commissioner again noticed an increase in the number of appeals. In 2013, the Information Commissioner dealt with only one appeal case in this area, four in 2014, eight in 2015 and already 16 cases in 2016. The Information Commissioner calls upon the bodies liable that they decide in favour of transparency and with special care when deciding on environmental information. This is because these issues attract a lot of publicity, as environmental information is relevant to a wide range of people, and the disclosure of such information is always in the public interest. Slovenian legislation sets the highest standards of transparency for environmental information and allows basically no legal exceptions when it comes to the publicity of such information.

The year 2016 was also marked by the adoption of the Amendment ZDIJZ-E, which is in force since May this year. The amendment brought changes especially to the field of re-use of public information, inter alia, by expanding the circle of bodies liable for the re-use to museums, libraries and archives. In 2016, with regard to the re-use, the Information Commissioner conducted four complaints procedures, which is more than in 2015 (when it conducted only one). According to the Information Commissioner's assessment, the applicants, i.e. the potential re-users, are well aware of their legal options in the event of the rejection of their application for the re-use. However, the complaint procedure itself (which is linked to the subsidiary use of ZUP) is too complex and lasts too long for their needs. The Information Commissioner therefore welcomes the solution incorporated by the Article 10.b of the Amendment ZDIJZ-E. Namely, the legislator instructed the bodies liable to proactively publish open data for the re-use online and to the Open Data Portal, when there is no obstacle for the free re-use of such data and which raise the most interest among potential re-users.

3 WORK IN THE FIELD OF PERSONAL DATA PROTECTION

3.1 Activities in the field of personal data protection

In Slovenia, the individual's right to protection of personal data is one of the constitutionally guaranteed human rights and fundamental freedoms. Article 38 of the Constitution of the Republic of Slovenia provides that the relevant criteria for collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided for by law. On that basis, the National Assembly adopted the Personal Data Protection Act of the Republic of Slovenia on 15 July 2004, which entered into force on 1 January 2005. The amended Personal Data Protection Act (ZVOP-1) was adopted in July 2007 and the consolidated text was issued on September 2007 (Official Gazette of the Republic of Slovenia, no. 94/2007). The purpose of the ZVOP-1 is to define, in a uniform manner, the rights, obligations, principles, and measures by means of which unconstitutional, illegal, and unjustified interferences with privacy and dignity of individuals in the processing of personal data are to be prevented. All other (sectoral) laws must be in line with these principles, and must clearly determine which personal data filing systems are to be established, which specific types of personal data they will contain, the manner of collection, the retention periods, possible limitations of individuals' rights and, in particular, the purpose of processing the collected personal data. Finally, in Part VI, the ZVOP-1 is also a type of sectoral act, defining the obligations of data controllers in the fields of direct marketing, video surveillance, biometrics, recording entry to and exit from the premises, and the supervision.

The Information Commissioner is entrusted with the enforcement of the ZVOP-1. In doing so, the Information Commissioner in 2016 conducted a total of 683 inspection cases of suspected violations of the Act. 245 of those cases concerned suspected violations in the public sector and 438 in the private sector. The Commissioner initiated 211 cases against legal persons of the public sector on the basis of reports received and 34 cases ex officio in accordance with the planned inspections or if, for example, publications in the media raised the Commissioner's suspicion of violations of data protection. The Commissioner initiated 390 cases against persons liable from the private sector, on the basis of reports received, and 48 cases ex officio.

The Information Commissioner conducted inspection proceedings with regard to the suspected violations of the provisions of the ZVOP-1:

- Unlawful disclosure of personal data: disclosing personal data to unauthorised users and unlawful publication of personal data – 185,
- Abuse of personal data for direct marketing purposes – 106,
- Unlawful collection or requiring of personal data – 99,
- Unlawful video surveillance – 61,
- Inadequate security of personal data – 40,
- Cookies – 37,
- Unauthorised access to personal data – 27,
- Processing of personal data contrary to the purpose for which they were collected – 23,
- Miscellaneous: processing of personal data after the retention period has expired; processing of personal data that is inaccurate and not up to date, refusing access to personal data; refusing the erasure of personal data – 38.

In addition, the Information Commissioner initiated 67 inspection procedures ex officio, in which it controlled the implementation of the provisions of the ZVOP-1 as a whole.

Within the framework of the above inspection procedures, 145 on-site inspections were carried out in total; 54 in the public and 91 in the private sector. Additionally, 68 inspections of websites were carried out. In order to address the established irregularities, the Information Commissioner issued a total of 144 measures (55 in the public and 89 in the private sector) in the form of warnings on the record, preliminary decisions, regulatory decisions or oral warnings.

Due to violations of the provisions of the ZVOP-1, 83 minor offence proceedings were initiated in 2016 (104 in 2015 and 95 in 2014), of which 41 were against legal persons from the public sector and their responsible persons and 13 were against legal entities in the public sector and their responsible persons. 29 proceedings were against individuals.

In minor offence proceedings, including those initiated in the previous years, the Information Commissioner issued 7 warnings and rendered 80 minor offence decisions (44 fines and 36 cautions). Furthermore, the Information Commissioner issued 62 additional warnings for minor violations (14 in the public and 48 in

the private sector), which is in line with the principle of procedural economy. In response, the suspected offenders filed a total of ten requests for judicial protection. The highest number of violations concerned the issue of inadequate security of personal data (52), unlawful processing of personal data (46), infringement of direct marketing provisions (20), unlawful video surveillance (19), unlawful purpose of collecting and further processing of personal data (18), and irregularities with regard to the establishment of filing system catalogues and supplying the catalogues to the information commissioner for the inclusion in the register of filing systems (9).

In 2016, the Information Commissioner received a total of five decisions of the local courts on requests for judicial review pertaining to this and past year's decisions. In two of those cases the court reduced the imposed fine, in one it dismissed the request for judicial review as unfunded, in one the court annulled the Commissioner's decision and closed the minor offence proceedings, and in one the proceedings were partially closed due to the statute of limitations and partially the case was dismissed as unfounded.

The Information Commissioner issued 1,330 written opinions or referrals to opinions already issued. In addition, state supervisors answered 1,884 questions over the telephone (there is a State supervisor on duty every working day). This means that all together, the Information Commissioner advised more than 3,200 individuals. The Information Commissioner published approximately 2,500 opinions on its website, which allows the individuals to find answers to their many questions. The opinions are classified into 47 fields (e.g. banking, biometrics, employment relations, e-mail, transfer of personal data to third countries, media, modern technologies, direct marketing, housing and real estate law, statistics and research, world wide web, education, video and audio surveillance, access to personal data, insurance, security of personal data, health data).

In 2016, the Information Commissioner received four applications (in 2015 there were six and in 2014 there were four applications) for issuing the decision on permissibility of implementing biometric measures. The Commissioner issued six decisions (two in cases transferred from 2015), in two cases it granted the request for the implementation of biometric measures, in one case it partially granted the request and in three cases it rejected applications:

- The Information Commissioner authorized the applicant to implement biometric measures for ensuring security of property using fingerprint readers to authorise certain employees to enter the pre-treasury and vault premises in the counting centre. The Information Commissioner assessed that the property that the investor wishes to protect by implementing biometric measures is so important that the need for protection outweighs the interference with the information privacy of the employees. The Commissioner took into account the gravity and the extent of the consequences that would have been caused by theft or other interference with the protected property, and the fact that the proposed implementation of biometric measures respects the principle of proportionality, as the measures will only be implemented over a narrow circle of employees.
- The Information Commissioner authorized the applicant to implement biometric measures for the purpose protecting business secrets using fingerprint readers to authorise entrance of members of the management board and their business secretaries. The offices of the management board members is where data is allegedly handled and stored and documents with different types and levels of confidentiality are created (e.g. confidential customer data in accordance with the Banking Act as business secrets). The consequences of unauthorized access and appropriation of data would be disproportionately greater and graver than the invasion into the information privacy of employees. In addition, the measures would be implemented exclusively over a narrow circle of executives and their business secretaries in accordance with the principle of proportionality.
- The Information Commissioner partially granted the applicant's request and, for ensuring the security of the property, authorised the implementation of biometric measures using fingerprint readers to authorise employees to enter two specially protected system spaces ("the bunker"), which include servers hired by customers (e.g. the telecommunications operators and banks) to store their data. The Information Commissioner took into consideration that ensuring the adequate level of security of equipment and data is one of the main reasons why the clients decide to trust the applicant to store their property with him, so the applicant is entitled and obliged to take and implement certain measures. The Information Commissioner rejected the application in part that referred to the intended implementation of biometric measures on individuals who are not employed by the investor, because such biometric measures are prohibited by the law.
- The Information Commissioner rejected the request of the applicant who intended to implement

biometric measures using fingerprint readers to control the entrance of the employees and outside associates into the director's office, financial and accounting departments and commercial offices. The purpose of the intended measures was to ensure the protection of classified information, business secrets and property. Upon examining the applicant's statements, the Information Commissioner found that there are in fact business secrets and property in those premises that need protection. However, the Commissioner concluded that the applicant did not demonstrate that the biometric measures are strictly necessary to protect those legal goods nor did he demonstrate that the protected goods cannot be protected with less intrusive measures.

- The Information Commissioner rejected the applicant's request to implement biometric measures for the purpose of performing his activities. The applicant stated that he would like to introduce these measures in the framework of upgrading or replacing of the system for registration of working time. The applicant's employees supposedly suggested that he installs fingerprint readers as they are allegedly simpler and faster to use than carrying around the cards. The Information Commissioner found that the applicant did not demonstrate how the performance of his activity could be compromised if he did not implement biometric measures for the registration of working time. Moreover, the applicant explicitly stated himself that the introduction of biometric measures is not strictly necessary. In addition, the biometric measures cannot be implemented on the basis of employee's consent, as was the proposed idea of the applicant.
- The Information Commissioner rejected the applicant's request, who intended to implement biometric measures for recording the workplace attendance. The applicant had discovered instances of abuse of the current system of recording the attendance. The Information Commissioner found that the applicant did not demonstrate that implementing biometric measures is strictly necessary, i.e. that he would not be able to carry out his activities properly if he did not record the attendance of his employees exactly with the use of biometric measures. The Information Commissioner also emphasised that the use of biometric measures does necessarily guarantee to the employer that employees were present at the working place during the registered working hours. Biometric measures are even less a proof that employees had properly performed his tasks.

In 2016, the Information Commissioner received 53 applications (in 2015 it received 14 applications) for the transfer of personal data to third countries. 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.

The Information Commissioner issued 52 decisions, by which it authorized data transfers to all the applicants:

- The Commissioner allowed 35 companies to transfer personal data to data processors in third countries on the basis of the provisions of contracts on data processing and taking into consideration the standard contractual clauses. The data that was intended for the transfer was information on employees and their family members, individuals who work on the basis of other civil contracts, job applicants, business partners, health professionals, pharmacists and patients involved in clinical research, participants in prize competitions and users of different websites and applications. The stated purposes for data transfer provided by companies were, for example, managing employee records, recruitment planning, managing the system of safety and health at work, providing helpdesk, providing analytical services for marketing activities, server maintenance, data centre transfer and centralization of IT services management, managing incidents and problems, implementation of biomedical research, monitoring of pharmacovigilance, cloud services, centralized data storage, mobile application performance.
- The Commissioner allowed 13 companies to transfer to third countries personal data of employees (former and current) and their relatives, personal data of other staff (trainees, students, volunteers), job applicants and personal data of clients or business partners for the purposes of human resources management and for the purposes of centralised HR policy and for the purposes of implementing centralised business, information and technical policy in order to increase the efficiency and improve the services. The Information Commissioner established that the exporter and importer of data belong to the same international group of associated companies. The legal basis for the transfer of personal data of employees is Article 48 of the Employment Relationships Act, as data transfer was necessary in order to exercise the rights and obligations

arising from the employment relationship, while the legal basis for the transfer of other personal data is consent.

- The Information Commissioner allowed three companies on the basis of the binding corporate rules (BCRs) to transfer and transmit personal data to data processors and data controllers in third countries within the groups which they are members of. Personal data allowed to be transferred was the following: data of employees, individuals who work on the basis of other civil contracts, job applicants, sellers and suppliers, health professionals and subjects of clinical trial and Internet users. The purpose of transfer was the employment and human resources management, keeping the internal directory of the group, the IT systems development and management, the promotion and assessment of products and services, service payments and reimbursement of costs, carrying out biomedical research or clinical trials, and providing user-friendly website experience.
- The Information Commissioner received a proposal from a pharmaceutical company to initiate a procedure for determining the appropriate level of protection of personal data in the State of Israel. The European Commission issued a decision on the appropriate level of personal data protection No. 2011/61/EU; the Commissioner is bound by this decision in its decision-making procedure. On this basis, the Information Commissioner decided that the State of Israel ensures an adequate level of protection of personal data in connection with automated international transfers of personal data from the EU or non-automated transfers where further automated processing is carried out in the State of Israel.

In 2016, the Information Commissioner received four applications (it received nine in 2015 and 14 in 2014) to connect personal data filing systems. The Commissioner issued three decisions granting the connection of personal data filing systems and issued one decision to stop the proceeding because the applicant withdrew his application.

The Information Commissioner issued the following decisions on connecting personal data filing systems:

1. It allowed the Ministry of Labour, Family, Social Affairs and Equal Opportunities to connect the filing systems that control personal data in the framework of the ISCSD (Information System of Social Work Centres) directly with the Tax Register IDIS_REK, whose controller is the Ministry of Finance - Financial Administration of the Republic of Slovenia. The connection between the filing systems is carried out on the basis of the EMŠO number (i.e. the personal identification number).
2. It allowed the Health Insurance Institute of Slovenia to connect the Register of insured persons under the compulsory health insurance with the Business Register of Slovenia, which is controlled by the Agency for Public Legal Records and Related Services. The personal identification number of the citizen (EMŠO) or tax number shall be used as the connecting code.
3. It allowed the National Institute of Public Health to connect the Central Patients Register via a direct computer link with:

- The Central Population Register and the Civil Registry, whose controller the Ministry of the Interior;
- The Register of insured persons under the compulsory health insurance, whose controller is the Health Insurance Institute of Slovenia;
- Personal data filing system on insurance policy holders and insured persons, whose controller is Vzajemna zdravstvena zavarovalnica, d.v.z.;
- A collection of data on insurance policy holders, insured persons, payers of contributions and beneficiaries of insurance payouts, whose controller is Triglav, Zdravstvena zavarovalnica, d.d.;
- The collection of data on insured persons, whose controller is Adriatic Slovenica, d.d.;
- A direct computer link between data filing systems may be achieved using the EMŠO or the compulsory health insurance number (ZZZS number).

In 2016, the Information Commissioner received 91 appeals in relation to the right to access personal data. This is a reason for concern especially because the number of applications increased by almost a third compared to previous years (there were 100 such complaints 2015 and 67 in 2014). The Information Commissioner also dealt with appeals on the count of individuals not being able to obtain health documentation under the Patient Rights Act (ZPacP). There were 15 such complaints (16 in 2015 and five in 2014). After examining the appeals, the Commissioner found that comparing to previous years, the share of administrative silence, that is when data controllers do not respond to the individuals' requests for access to personal data, was 32%, which is about the same as in 2015 when the share was 33%. In 2014, the share was 49% and in 2013 52 %. The appeals lodged in 31 cases concerned State bodies (mostly ministries, bodies affiliated to ministries and courts), 15 appeals concerned healthcare institutions, six cases involved centres for social work, four cases banks and three cases educational institutions. The rest of the complaints concerned various data

controllers (such as societies, insurance companies, telecommunications operators). In 37 cases, data controllers reacted immediately to the Information Commissioner's call to grant the individuals' right to inspect and obtain the requested information or provided them with an explanation as to why they refuses this right. The Information Commissioner issued ten decisions whereby it granted five complaints in full and five complaints in part. Nine data controllers executed the Commissioner's decisions, and one decision was challenged before the Administrative Court of the Republic of Slovenia. The Information Commissioner also issued 11 rejection decisions in complaint cases against controller's and dismissed ten appeals on procedural grounds (one due to the lack of its competence and the other because the individual did not supplement his application after being urged to do so). The Commissioner advised 23 individuals on how to proceed in their case and referred three complaints to the competent authorities.

The Information Commissioner also dealt with three complaints concerning the right to supplement, correct, block, erase and object. Three applicants requested that the Information Commissioner prohibits disclosure of their personal data to a certain data controller (i.e. the manager of multiple dwellings) and to two individuals. The applicants stated that the manager and some individuals unlawfully disclosed their personal data by distributing the decision of the Information Commissioner, without redacted personal data, to third parties. The individuals demanded from them that they stop processing their personal data unlawfully. The Information Commissioner first found that first names and addresses of the applicants were redacted from the decision, while the family names and street addresses were still visible. This led the Information Commissioner to decide that the decision at hand was not anonymised, because the individuals were identifiable. However, in the specific case, the applicants cannot exercise the right to supplement, correct, block, erase and object, because they seek a ban on unlawful processing in the future, while the rights mentioned relate only to the ongoing processing. The individuals may seek from the court a declaration of unlawfulness and compensation for the past processing claim. The Information Commissioner, on the other hand, was competent for conducting the inspection procedure due to disclosure of non-anonymised decision and it found that the manager and the two persons had no proper legal basis for the disclosure of the decision. However, due to the nature of the violation found, the Commissioner could not order that personal data should not be processed in the future. It did however initiate a minor offence procedure for the past violation. On the basis of the above, the Information Commissioner concluded that the applicants' claims were not justified and their applications were rejected.

In 2016, the Information Commissioner did not file any requests for a review of the constitutionality, but it did receive a judgment of the Constitutional Court of the Republic of Slovenia in relation to the request filed in April 2013. The request concerned the question of the constitutionality of the provisions of Paragraphs 1, 7 and 8 of Article 20 of the Tax Procedure Act (ZDavP-2), which determine the obligation to publish on the Internet a list of individuals who failed to pay their tax obligations. The Information Commissioner found during the inspection procedure that personal data of individuals (name, date of birth and the "class" corresponding to the amount of defaulted tax payments) were published on the websites of the Tax Administration of the Republic of Slovenia and the Customs Administration of the Republic of Slovenia. It was also found that these data were published in accordance with the law and therefore the Commissioner could not order that they be taken off the Internet. The Information Commissioner stated in the request for a review that the impugned provisions do not pass the so-called stringent proportionality test as the measure of publication of personal data was not necessary and appropriate to achieve the objective of voluntary payment of taxes or an improvement of the country's culture of paying taxes. Moreover, the Commissioner assessed that the publication of the list of tax debtors is inconsistent with Article 22 of the Constitution of the Republic of Slovenia (equal protection of rights), since individuals did not have adequate legal protection in case of unjustified public disclosure of their personal data. This is due to the fact that the Internet practically never forgets the information that is once published. The individual is not specifically informed prior to publication that his data will be published nor does he have the opportunity to give a statement on whether the debt had been accurately identified and why was the debt created. The Constitutional Court did not follow the Commissioner's arguments in the request for the review and, by decision Ul-122/13-13 of 10 March 2016, found that the ZDavP-2 in the challenged part is not inconsistent with the Constitution. Thus, the publication of tax debtors (who are natural persons) is constitutionally permissible. The Constitutional Court judges dr. Dunja Jadek Pensa and dr. Jadranka Sovdat, however, pointed out in their dissenting opinion that the matter concerns the publication of data from non-final tax decisions, which, according to the Information Commissioner, leads to public stigmatisation of individuals. The General Financial Office publishes once a month data on tax debtors who are natural persons and who owe more than EUR 5,000 for more than 90 days. It publishes the debtor's name and date of birth, and the data are classified into classes according

to the amount of outstanding unpaid tax debt. Although the Information Commissioner does not share the opinion of the Constitutional Court, it will, naturally, respect the Court's decision.

3.2 Selected cases involving a violation of personal data protection

3.2.1 Video surveillance of the driveway

An individual supposedly installed a camera which records the driveway used by several families.

The Information Commissioner found that all the roads in the immediate vicinity of the individual's house are privately owned. The Commissioner concluded that an individual is conducting a video surveillance for personal use and is not bound by the provisions of the ZVOP-1 as provided by Paragraph 1 of Article 7 of the ZVOP-1. Thus, the Information Commissioner is not competent to act. The Commissioner could act only if the individual would also record a public area (judgment of the Court of Justice in the Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů).

In accordance with Article 134 of the Obligations Code,[23] the injured person may file a lawsuit before a court which may order that the act (of video surveillance) be ceased if it violates the inviolability of the person's personality, private and family life or some other personality right. In the event that such video surveillance or displaying the recordings result in material or non-material damage, the injured person may, pursuant to Article 179 of the OZ, claim compensation from the person causing the damage. Unlawful visual recording is also a criminal offense under Article 138 of the Criminal Code.

Video surveillance over private property, if not carried out by a business entity, therefore does not fall within the competences of the Information Commissioner.

3.2.2 Collecting personal data for the purpose of recovery of parking fees

The Information Commissioner received several reports on the alleged unlawful acquisition of personal data for the purposes of recovering fines and unpaid parking fees abroad. The Commissioner initiated an inspection procedure against the law firm that acquired and transmitted personal data of motor vehicles owners or users.

The Information Commissioner found that the conditions for acquiring personal data pursuant to Article 10 of the Attorneys Act (ZOdv)[24] were not met. In accordance with this Article, lawyers may acquire personal data from statutory designated controllers (State bodies, local government bodies and public power holders) only when this information is required in the performance of the lawyer's profession in a particular case. Lawyers may not exercise this right to acquire personal data for the client without having a basis at the time of acquiring data in the explicit purpose (and the client's order) to perform a concrete act of legal representation for which information is needed. In the particular case, the law firm provided the acquired personal data to the client without any other purpose, because the data was not needed for the legal representation. The Commissioner assessed the agreement by which the lawyer acquires personal data and transmits it to the client who then uses the data on his own to try and recover the debt from a debtor whose identity was discovered by the lawyer and only later possibly hires the lawyer for the recovery of debt. The Commissioner established that such an agreement does not justify the acquisition of data according to the provision of Article 10 of the ZOdv.

The Information Commissioner found that the law firm acquired most of the personal data unlawfully, because it did not and will not need such personal data in the course of exercising the lawyer's profession. The Commissioner ordered the law firm to stop the acquisition of personal data in such cases and ordered the erasure of all unlawfully acquired personal data.

Nevertheless, the Commissioner noted that the individuals are not exempt from paying the debt even though their personal data may have been acquired unlawfully. This is because the creditors from abroad (legally) possess the information on the vehicle's registration number, which enables the identification of the alleged debtor lawfully at any time.

[23]Official Gazette of the Republic of Slovenia, no. 97/2007 – official consolidated text 1; hereinafter the OZ.
[24]Official Gazette of the Republic of Slovenia, no. 18/1993 with amendments; hereinafter the ZOdv.

3.2.3 The use of a body scanner at the airport

A body scanner was allegedly used without prior notice and personal consent of individuals for performing passenger control at the entrance to the passenger terminals.

The Information Commissioner found that the person liable was testing a security scanner operating on the principle of non-ionizing millimetre waves. The person liable explained that when scanning a 3D model of an individual is drawn up and areas where illegal materials might be located are marked. The device stores the 3D model temporarily; it does not, however, show it to the investigator directly, but in the form of two 2D projections of the generic silhouette of a person (one from the front and one of the rear). On this silhouette, the areas where an unusual reflection of waves occurs are marked with squares. If the device does not detect unusual reflections, the scan is complete; otherwise the scan is repeated or complemented with the manual examination. After that, the image that had been saved is discarded. This means that neither the original 3D models nor the simplified 2D models are saved. When entering through the device, a written notice was installed that "the scan is performed with a security scanner that uses the so-called millimetre wave technology for security". Therefore, an individual could refuse the use of the scanner and in this case, he would be subject to manual examination only.

The Information Commissioner concluded that the person liable does not violate the provisions of the ZVOP-1 by using a security scanner. This is because the use of the scanner does not result in processing more personal data than it did prior to the use of the scanner. Therefore, the Commissioner closed the inspection procedure.

3.2.4 Insufficient security of personal data of users of services on telecommunication operator's servers

The telecommunications operator (hereinafter referred to as the person liable) allegedly failed to adequately secure personal data of users of its services by keeping access to the personal data of the users of the services on two servers unsecured. This supposedly resulted in the publication of an open and freely accessible database "Elasticsearch", which contained mail server journal entries. In addition, a freely accessible cache of the "Memcached" related web application was allegedly located in one of the servers of the person liable, disclosing e-mail addresses of recipient and / or senders of messages, time stamps and IP addresses.

The Information Commissioner found that the person liable did not respect Articles 24 and 25 of the ZVOP-1. Namely, the person liable kept personal data of more than 8,000 individuals unsecured for a certain period of time on its two mail servers (the data being the e-mail addresses of senders and IP addresses from which messages were sent, e-mail addresses of the recipients, dates and times of their sending). Access to the above mentioned personal data was possible through the use of the remote access protocol "Telnet", which enabled the "entry" into mail servers of the person liable through specified open ports. This was due to the fact that the person liable did not ensure that the firewall activated in case of an unforeseen temporary shutdown of the server due to overheating. In addition, the security settings were not regularly checked by the person liable and it never implemented restrictions on access to mail servers with the use of authentication or other appropriate methods of permanent personal data protection. Anyone who remotely connected to the mail servers could have copied these unsecured personal data, but because the person liable failed to provide proper traceability of the processing, personal data is being processed in an unauthorized, untraceable and uncontrolled manner still to this day.

Therefore, the Information Commissioner initiated a minor offence procedure against the person liable. When this procedure becomes final, the Information Commissioner will also be able to end the inspection procedure.

The procedure also established a suspicion that the person liable violated not only the provisions of the ZVOP-1, but also the provisions of the Electronic Communications Act, as the operator did not take the appropriate technical and organizational measures for managing the risks to the security of networks and services. For this reason, the Information Commissioner transferred the report in this part, together with its findings, to the body, competent for monitoring the implementation of the Electronic Communications Act (ZEKom-1).

3.2.5 Inadequate security of personal data of patients and employees on the website

The person liable allegedly inadequately secured personal and sensitive personal data on its website. It was alleged that with merely entering a particular URL link into the web browser it was possible to access sensitive personal data, including the diagnosis of individual patients.

The Information Commissioner found that entering the specified URL link to the web browser enabled unsecured access to a large number of health and other documentation. Entering the link also enabled unsecured access to personal data of a larger number of employees at the person liable.

The person liable was informed by the Information Commissioner of the security incident the same day and it was urged to secure access to data on the website as soon as possible in such a way as to prevent unauthorized persons from accessing personal data. The person liable stated that it set up an intervention team of experts and informed the SI-CERT of the incident.

The person liable eliminated the irregularities that had been discovered, so the Information Commissioner closed the inspection procedure. The Commissioner did however impose a fine on the person liable and its responsible person due to the inadequate protection of sensitive personal data of patients and personal data of employees, namely, for the violations of Articles 24 and 25 of the ZVOP-1.

3.2.6 Illegal acquisition of personal data for the purpose of direct marketing

The director of the person liable allegedly used a database of e-mail addresses owned by a company where he worked prior to establishing his own company (the person liable) for the purposes of direct marketing.

The Information Commissioner found that the person liable used the database for direct marketing purposes and for this purpose it processed personal data of natural persons, namely their names, surnames and e-mail addresses. In this database for direct marketing, there were nearly 1,000 e-mail addresses, of which 850 were supposedly acquired from web sources, while the rest were acquired through conducting his business, personal acquaintances and other sources. The Information Commissioner did not follow such an explanation, as the person liable was unable to demonstrate for a majority of these e-mail addresses, which were randomly selected from the database, that they were available on the Internet. In addition, with the exception of one e-mail address, the context of the publication of other e-mail addresses is in no way related to the performance of the activities of the person liable. The Information Commissioner also ruled out the possibility that the director of the person liable memorised such a large number of clients which he got knowledge of on the basis of his experiences and acquaintances in the course of working at the previous company as a student, and to obtain their contact information (e-mail addresses) from publicly available sources.

The director of the person liable did not acquire e-mail addresses, used for direct marketing, online, but it had copied illegally the database containing personal data from the company in which he had worked in the past. The person liable should have a proper legal basis for storing and using these email addresses for direct marketing, namely the individuals' consent. In the course of the procedure, the person liable obtained the consent of 98 individuals to use their e-mail addresses to send advertisements, while it deleted all other e-mail addresses of natural persons from the database. By doing so, the person liable eliminated the irregularities; therefore the Information Commissioner closed the inspection procedure and initiated the minor offence procedure. With such conduct, the person liable, namely its director, violated Article 8 of the ZVOP-1, which was the reason for the Information Commissioner to impose a fine.

3.2.7 Disclosure of information regarding personal bankruptcy on the envelopes

The Information Commissioner initiated two inspection procedures due to the suspicion of unlawful disclosure of information regarding personal bankruptcy of individuals on the envelopes. The two persons liable supposedly wrote their remark on the outer side of the envelopes saying "IN PERSONAL BANKRUPTCY" beside the name and surname of the addressee (an individual who was in personal bankruptcy). By doing so, they allegedly interfered with the individuals' (information) privacy and violated the provisions of the ZVOP-1.

In the first inspection procedure, the Information Commissioner found that the person liable (a supplier of utility services) wrote a remark "IN PERSONAL BANKRUPTCY" on all the deliveries it sent directly to the insolvent debtor. The individuals were supposed to notify the person liable on their payment (in)ability or personal bankruptcy on the basis of the utility services supply contract. However, due to the inconsistency in fulfilling their contractual obligation, the person liable was obliged to obtain these data from the publicly available AJPES register by itself. The person liable justified its conduct with the fact that the personal bankruptcy data are publicly accessible through the AJPES portal. However, the Information Commissioner explained that the Financial Operations, Insolvency Proceedings and Compulsory Winding-up Act (ZFPPIPP)[26] declares that a simple search for an insolvent individual only by entering his personal name is not allowed and neither does the AJPES enable such a search. The ZFPPIPP limited the search options regarding personal bankruptcy data precisely to protect the individuals' privacy.

The Information Commissioner concluded that in accordance with Articles 24 and 25 of the ZVOP-1, the person liable was obliged to ensure the security of information on personal bankruptcy even during postal deliveries. This should have been achieved either by preventing the remark "IN PERSONAL BANKRUPTCY" to be printed on the envelopes or by deleting it before the delivery is sent. Due to the unlawful disclosure of personal data, the Commissioner initiated a minor offence procedure against the person liable and its responsible person. The Commissioner also stopped the inspection procedure, as the person liable permanently prevented the printing of the remark regarding personal bankruptcy on the envelopes and documents.

In the second inspection procedure, the Commissioner found that despite the clear internal instructions for the employees, an error occurred when entering data into the database of the person liable (a bank). Consequently, a customer of the bank was sent a delivery with the contested remark regarding personal bankrupcy. When the costumer warned the person liable, the latter immediately deleted the controversial personal information from the name field.

The Information Commissioner concluded that the person liable did not provide adequate security of personal data of the customer and thus violated the provisions of Point 3, Paragraph 1 of Article 24 and Paragraph 1 of Article 25 of the ZVOP-1. The Information Commissioner imposed a measure in accordance with the ZP-1, and stopped the inspection procedure when the person liable demonstrated that it eliminated the error it had caused.

[26]Official Gazette of the Republic of Slovenia, no. 13/2014 – official consolidated text 1, with amendments; hereinafter the ZFPPIPP.

3.2.8 Unlawful disclosure of personal data relating to the charging of copying costs

The person liable allegedly disclosed personal data of secondary school students unlawfully to a private photocopying service provider for the purpose of preparing an estimate of costs for photocopies of non-compulsory school materials.

The Information Commissioner found that the person liable is a controller of personal data of students and their statutory representatives who did not expressly oppose the method of payment. Therefore, the person liable sent a complete table with personal data (name, surname, address) of all 770 students and 1,470 of their statutory representatives to the photocopying company for the purpose of receiving offers or estimates of annual photocopying cost. The individuals were not informed of this beforehand. The Information Commissioner concluded that the person liable had no legal basis for the disclosure of personal data to the photocopying company. Therefore, the Information Commissioner initiated a minor offence procedure against the person liable and its responsible person. The Commissioner also closed the inspection procedure because, in the present case, the disclosure of personal data filing system was a one-off act in the past, which an inspection measure could not retroactively prevent or eliminate.

In the procedure against the photocopying service, the Information Commissioner found that personal data of students that the company obtained from the person liable was used to issue estimates of photocopying costs for the school year 2015/2016. As a legal basis for such processing of personal data, the company referred to Point 5, Paragraph 1 of Article 82 of the Value Added Tax Act (ZDDV-1),[27] which provides that a taxable person issuing an invoice must provide the following information on the account: the name and address of the taxable person and its buyer or subscriber.

The Information Commissioner concluded that the said provision of the ZDDV-1 was not a proper legal basis for obtaining and further processing of personal data of all students and their statutory representatives. This is because the photocopying company did not demonstrate that at the time of obtaining the said personal data there was already an established obligatory relationship between the company and individual student as a subscriber or buyer of photocopying services. In accordance with Article 28 of the Obligations Code (OZ),[28] such a relationship was established with the acceptance of the offer (i.e. by paying the estimate), which in turn represented a legal basis for issuing an invoice in accordance with the provision of Article 82 of the ZDDV-1. 768 students paid the estimates to the company and were issued an invoice. Two students did not pay the estimates, which means that they did not accept the company's offer and consequently their personal data were kept unlawfully in the company's filing system. Considering the fact that all the estimates and invoices were issued in the students' name and not in the name of their statutory representatives, the Information Commissioner further concluded that the photocopying company processed personal data of all the 1,470 statutory representatives (acquired and further retained) without any need and without due consideration of the principle of proportionality. Furthermore, the company had no legal basis from Article 10 of the ZVOP-1 for processing of personal data. Therefore, the Information Commissioner ordered the photocopying company to erase the unlawfully obtained and retained personal data of the two students and of all the statutory representatives. The photocopying company completely and permanently deleted the data and enclosed the proof thereof to the Commissioner. The latter thus found that the violations of the ZVOP-1 have been eliminated and closed the inspection procedure.

[27]Official Gazette of the Republic of Slovenia, no. 13/2011 – official consolidated text 3, with amendments; hereinafter the ZDDV-1.
[28]Official Gazette of the Republic of Slovenia, no. 83/2001 with amendments and supplements; hereinafter the OZ.

3.3 General assessment of the status of personal data protection and recommendations

In 2016, the Information Commissioner in relation to the implementation of inspection supervision in the field of personal data protection, handled:

- 683 inspection cases, of which 245 in the field of the public sector and 438 in the private sector; and
- 83 minor offence procedures.

In addition to inspection and offence procedures, the Information Commissioner received and handled in the year 2016:

- 1,330 requests to issue a written explanation or an opinion in relation to specific questions;
- Four requests for a decision on the permissibility of connecting data filing systems;
- Four requests for a decision on the permissibility of implementing biometric measures;
- 53 requests for authorisation of the transfer of personal data to third countries;
- 91 appeals regarding the right to access data subject's personal data; and
- Three appeals regarding the rejection of the request to cease with the processing of personal data.

Of the 683 inspection cases that the Information Commissioner handled in 2016, 601 were initiated on the basis of a report, and 82 were initiated on the Commissioner's initiative. In the public sector, 211 reports and complaints were filed and in the private sector 390. 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, the use of personal data for the purposes of direct marketing, on redirecting and consequently reading e-mails received by employees on their company's e-mail address, on implementation of video surveillance systems, on to the publication of personal data on websites, and on inadequate security of personal data.

As in the previous years, the Information Commissioner found in 299 out of 601 examined reports 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 share of such reports was 49%. 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.

Among the reports, complaints and applications filed with the lack of knowledge of the competence of the Information Commissioner, it is worth highlighting those that relate to the collection and use of personal data in judicial and administrative proceedings. In such cases, the Information Commissioner sends to the applicants a notification that it will not initiate the inspection procedure. In the notification, the Commissioner explains that according to the decision of the Constitutional Court of the Republic of Slovenia, No. UI-92/12-13 of 10 October 2013, the Commissioner must not implement inspection supervision over the provisions of the ZVOP-1 in a way that, while the Commissioner exercises its statutory powers, it would interfere with individual legal procedures conducted by the competent state authorities. During the inspection procedure, the Commissioner is also not allowed to inspect whether constitutional and legal protection of personal data is afforded to individuals in individual legal proceedings.

In 2016, the Information Commissioner strengthened the implementation of the so-called planned ex officio inspections on the basis of the adopted annual plan. In this year, the planned inspections over the compliance with the provisions of the ZVOP-1 focused on the police, healthcare institutions, banks, savings institutions, consumer creditors, insurance companies, local self-government bodies, higher education institutions, secondary schools and energy companies.

As already stated in the Report for 2015, the last 10 years of the Commissioner's operations saw a significant improvement of both the general and the professional public's awareness of privacy and data protection.

As already stated in the 2015 Report, the awareness of both the general public and the professional public regarding privacy and the protection of personal data has improved significantly over the last ten years of the Information Commissioner's work. The main problems with knowing the legislation have been superseded, but we still observe deficiencies and irregularities at data controllers and processors in certain areas. It is worth mentioning here especially health information, which belongs to a category of sensitive personal data and should therefore enjoy the highest level of protection. Misuse of such information can have serious and long-lasting consequences for the individual, and any unauthorized processing is an interference with the fundamental patients' rights. Therefore, the Information Commissioner has continued to raise proper awareness and to carry out supervision in healthcare institutions, taking into account its available resources and the fact that its competencies spread throughout the entire public and private sector. The Commissioner has thus carried out on its own motion a significant number of inspections in hospitals and at other healthcare providers in the framework of the planned annual inspection supervisions. It is worth mentioning that 10 years ago, the traceability of access to health information was a rare occurrence, but the Commissioner's continued efforts in the inspection procedures and the measures it has ordered to healthcare institutions have significantly reduced the possibility of undetected access. Even though the situation in healthcare sector improved thanks to the findings and measures of competent monitoring authorities, we can still observe certain violations, most notably:

- Transmitting health information through unsecured (unencrypted) connections (via regular e-mail, unencrypted web links);
- Lending the means of authentication for accessing the data, such as passwords and cards, and their inadequate security,
- Leaking and selling data from healthcare institutions for the purposes of direct marketing,
- Limited transparency and control over data processing by external contractors,
- Insufficient awareness of the fact that disseminating patients' information might be inadequate,
- Insufficient securing of the premises in which health records are kept.

The Information Commissioner therefore called upon the controllers who process health information to verify the existing procedures and measures for data protection and adapt them. The Commissioner announced that it will continue and strengthen the supervision in over the healthcare institutions and other controllers of sensitive personal data.

It is also worth drawing attention to other frequently identified irregularities and deficiencies found by the Information Commissioner in all areas. This includes, in particular, the irregularities and deficiencies in managing up-to-date catalogues of personal data filing systems and consequently of supplying information for the Register of filing systems, and 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 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 processors, and redirecting and unauthorised reading of company e-mails.

The Commissioner's findings regarding video surveillance systems in the workplace and the use of recordings for the purposes of supervising the employees call for a warning regarding the increasing use of affordable IP cameras. These allow the managers of companies to access at any time via the Internet and by using a smartphone, a tablet or a personal computer, the so-called live stream that is shown by individual cameras, and thus supervise the work of employees, located at the premises that are being supervised. The Commissioner is convinced that such supervision of employees is inadmissible in terms of the proportionality of the invasion of privacy of employees. Video surveillance in the workplace may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by milder means. Taking into account the abovementioned strict conditions imposed by the law on the implementation of video surveillance in the workplace and the use of recordings, it is not permissible to directly access and monitor live stream cameras placed within work areas, except in cases where this is strictly necessary for the safety of people and property. Monitoring live stream cameras is only permitted for persons who are obliged, by the nature of their work, to constantly monitor the events covered by cameras in the protected area. These persons are, as a rule, security guards or persons in

the control centre, and are by no means managers who wish to check the live stream when they happen to have time or think it is necessary to see what is happening in a workspace. If we allowed managers to access live stream cameras, this would in practice mean, that they could always look at the live stream and monitor how employees perform their jobs. This would represent a disproportionate invasion of employees' privacy and a use of video surveillance systems for unlawful purposes.

With regard to the use of IP-cameras that connect internationally and are accessed through a computer, a tablet, or a smartphone, it should be noted that users often forget about securing the access to such cameras in an appropriate manner, which further increases the risks for the invasions of privacy. The Information Commissioner thus calls again upon the users of such devices, which are often used for domestic and private purposes, to verify that the access is limited at least with appropriate passwords, which must be complex and must differ from default factory passwords. Namely, in many cases, the access to video surveillance cameras that are connected to the Internet is insufficiently secured, which allows malicious and curious individuals to gain insight into the events occurring at the company's premises or even individuals' homes, without authorisation and the owner's knowledge.

It should be pointed out that the persons liable, as a rule, eliminate the abovementioned irregularities and deficiencies voluntarily on the basis of a warning issued to them by the National supervisor for the protection of personal data. For this reason, issuing a (regulatory) inspection decision is usually not necessary. According to the case law and the principle of the hearing of the party (Article 9 of the ZUP), the Information Commissioner is required, before issuing a decision ordering the cessation of processing or erasure of unlawfully acquired personal data, to provide prior information to the person liable on why it believes that the said processing of personal data is without proper legal basis and the arguments that confirm such a view. For all these reasons, the Information Commissioner issued only three regulatory decisions in 2016 by which it prohibited unlawful processing of personal data. It should be noted, however, that the voluntary elimination of the irregularities found does not relieve the person liable of the offense, criminal and tort liability. The Commissioner may still initiate a minor offence procedure or order measures in accordance with the law on minor offences, against the person liable and its responsible person, in the event that it discovers a suspicion of violation of the law.

In the past, the Information Commissioner constantly warned about the problem of imposing disproportionately high fines for the concurrent minor offences. The Commissioner suggested that a solution is found together with the experts from the Ministry of Justice, which would enable the Commissioner, in the case of concurrent offences of the same kind, to impose against an offender a single fine, which would be lower than the sum of fines, determined for a single offense. This need arose from the judgment of the Supreme Court of the Republic of Slovenia, No. IV Ips 51/2011 of 21 June 2011, regarding the concurrent minor offenses in the event of unlawful processing of personal data. The Supreme Court took the view that "in the case of such offenses there are as many offenses as there are injured parties" and that "each interference with the individual's right to information privacy constitutes an independent offense." This interpretation led to the Commissioner imposing disproportionately high fines in practice, as the Commissioner has no power to impose a single fine that would be lower than the sum of the lowest prescribed fine in cases of (real or ideal) concurrence when there is a large number of individuals whose personal data has been interfered with. The Information Commissioner thus imposed a single fine as high as EUR 1 million for medium and large enterprises and EUR 20,000 for the responsible persons of legal entities, sole proprietors and responsible persons of State bodies and local self-government bodies.

The Ministry of Justice took into account the initiative of the Information Commissioner in the preparation of the Amendment to the Minor Offenses Act (ZP-1J). Article 9 of the Amendment ZP-1J, which entered into force on 6 November 2016, stipulates that at the end of Paragraph 2 of Article 27, a new sentence is added which reads: "If justified by the circumstances from the second, third and fifth paragraph of the preceding Article, a single fine may be imposed on the offender for the offenses of the same type in concurrence for which one offense decision is issued (Article 56) and which does not reach the sum of certain sanctions or does not exceed the maximum amount of a particular type of sanction under this Act." Accordingly, from the entry into force of the Amendment onwards, the Information Commissioner may impose on the offender a single fine, which is lower than the net sum of the fines for a particular offense, in case of offences of the same type in concurrence. However, the Commissioner may only do so if the circumstances from Paragraphs 2, 3 and 5 of Article 26 of the ZP-1 justify it. The authorised official of the Commissioner must assess these circumstances on a case-by-case basis.

Persons liable who do not have business premises but operate only through a mailbox and persons liable who are represented by foreign nationals as registered in the Business register, still present a big problem in the process of inspection procedure. The majority of such persons liable deal with online sales and they collect and use personal data for the purpose of intrusive direct marketing. The current state of affairs enables these persons liable to act unlawfully and avoid liability for offenses committed, causing the Republic of Slovenia and its inhabitants significant economic damage. At the Commissioner's initiative, the issue was dealt with by the Inspection Council at the meeting held on 12 October 2016. A decision was made that the members of the Inspection Council will submit their proposals on how to improve the current situation regarding the problem of serving of the postal deliveries to representatives of companies who are foreign nationals. In addition, the Legal Affairs Committee of the Inspection Council will prepare a proposal and materials for the Ministry of Economic Development and Technology and the Ministry of Justice on the basis of the responses received.

In 2016, the protection of personal data in the European area faced a major turning point. On 4 May 2016 the two key data protection acts were published in the Official Journal of the European Union, namely:

- 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) and
- Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The General Data Protection Regulation (GDPR) entered into force on 25 May 2016 and its provisions will have direct application in all Member States within two years. The deadline for transposing the provisions of the Directive into national law is also two years.

Larger data controllers have already started to prepare themselves to the use of the General Data Protection Regulation, as certain adjustment activities needed to be started early enough. Namely, certain processes will need to be adapted, the appropriate staff will need to be engaged and existing levels of personal data protection will need to be assessed. The year 2016 was characterised by learning about the new provisions, while in 2017 there will be no more time for learning, but the State will need to decide how to implement the Regulation in the Slovenian legal order and how to regulate areas where Member States are afforded more freedom (e.g. rules on health, biometric and genetic data).

When assessing the level of awareness and knowledge of the concept of personal data protection and the legislative provisions, the Information Commissioner is of the view that the situation is good, but there are certain differences (depending on the industry, size of the controller, etc.). The general awareness of the importance of privacy and personal data protection among the public is moderate. The Commissioner's permanent and never ending task is to attempt to explain the importance of the right of self-determination, the long-term nature of certain measures and timely and comprehensive consideration of not just the positive aspects of new technologies, powers, regulations and systems. Without privacy, we cannot speak of a free and democratic society; therefore, we need to speak up when someone wants to abuse this right to hide something bad. This is not an easy task, as understanding privacy requires more than just understanding safety, economy and practicality, the three concepts that can be presented to the public with greater ease and in a populistic manner.

The field of smartphones is blooming, as they are becoming a single point for identifying an individual, a means for accessing different systems and services, and a replacement for other devices. Smartphones are becoming our wallets, they keep our loyalty cards, and a go-to device for accessing e-mail and social networking profiles. They enable the system of rewarding drivers according to their driving profiles, they unlock electric cars and lock and unlock hotel rooms. The possibilities offered by this device that is always at our side are endless. In turn, the circle of entities that collect data about us and use them for good or for bad is also expanding. In relation to smart devices, the General Data Protection Regulation recognizes the importance of various online identifiers, the risks of increasing profiling practices and automated decision-making processes. It establishes various requirements for preventive action of controllers, as it includes validation mechanisms, data protection officers, impact assessments, principles of privacy by design and

by default, and the principle of accountability. The Information Commissioner estimates that preventive and proactive approaches to privacy protection are positive, but they will certainly be a novelty for some controllers, who will have to accept it. The impact assessments and data protection officers has thus far been in the domain of only the largest controllers, such as banks, insurance companies and pharmaceutical companies. Now, the advantages of such preventive measures will spread to other data controllers.

Similar trends as identified in previous reports of the Information Commissioner continue in 2016: namely the accelerated digitization in all areas of life, i.e. the big data, profiling and development of artificial intelligence and the Internet of Things. Individuals are being profiled in all areas of life, while algorithms and artificial intelligence are increasingly taking the decisions about the individuals. These decisions have sometimes a small impact, which can be damaging or useful (for example, a decision on which ad will be shown to a particular individual), but they may also have an important impact (whether an individual will receive a scholarship, the conditions for granting the credit), if not a critical one (whether an individual is a suitable candidate for treatment with a specific, expensive medicine). While benefits of the trends promised by the big data and artificial intelligence are often praised, too little attention is paid to the dangers, for example of self-learning machines that make decisions about individuals that no one else can explain or dare to disagree with. Perhaps it sounds like science fiction now, but in ten years this reading will not be so futuristic.

Equally important areas are those of genetic and biometric data, which will be left to a greater discretion of the Member States by the General Data Protection Regulation in terms of preserving or establishing the rules. The main challenges with regard to the Internet of Things arise from the security field, because for many developers, securing new connected points is not a number one priority, but they connect more and more things to the Internet, whether this is sensible or not (e.g. smart lamps, refrigerators, sports watches and lately, increasingly, the cars). As in all other areas related to information and communication technologies, we must understand that ensuring security should not be a one-time act, but that security mechanisms should be properly designed, reviewed, updated and upgraded. However, the more devices that are connected, the more effort is needed. According to some estimates, up to 30 billion devices will be supposedly connected to the Internet in 2020, but we hear on a daily basis that there are already huge problems with the existing devices. Namely, even the largest controllers manage systems that are vulnerable, they log intrusions into their servers and face data loss.

No matter which trend we observe, it is important to remember that changes in the field of privacy are swift, gradual, and difficult to detect. Do you remember when loyalty cards were first introduced? What about digital TV? There are less and less areas where no personal information is being collected about us, but we hardly even notice it. Data is power, and this power is increasingly shifting from us to others - our traders, operators, the State, intelligence agencies, law enforcement agencies. We are becoming transparent to an increasing number of people and companies and thus our decision-making power is becoming weaker. We are only at the beginning of true mass data collection era, but the value and power of personal data are clearly reflected in the value of technological giants, the use of data for voters' manipulations and directing individuals' purchasing and other decisions. If not sooner, we will realize the value of privacy when we finally lose it.

In 2016, the Information Commissioner paid special attention to the preventive aspects of its operation. With the aim of educating controllers and other persons liable, the Commissioner's employees conducted 96 free lectures for domestic audiences, while this number exceeds 100 if we take into account the lectures given to foreign guests. The Information Commissioner is also in constant contact with data controllers, processors and proposers of regulations with the aim of timely addressing various dilemmas regarding new ways of collecting and processing personal data and searching for privacy-friendly legal solutions while introducing new technologies and increasing efficiency. Among other things, the Commissioner conducted lectures for experts of all existing ministries, who prepare laws and regulations that touch upon the protection of personal data. The Commissioner also prepared more than 120 opinions on proposals of laws and other regulations that refer to various aspects of managing, collecting and processing of personal data.

The Information Commissioner also assists informally with the performance of privacy impact assessments as one of the basic tools for a timely approach to an adequate protection of personal data. Again in 2016, more than 100 controllers and processors from the public and the private sector contacted the Information Commissioner in the process of drafting legislation and preparing solutions or projects, because they encountered dilemmas regarding personal data protection that they wanted to address appropriately before the implementation. The personal data protection impact assessments have a major preventive effect, as

fewer inspection measures are needed, fewer violations are found, and data controllers have lower costs due to imposed sanctions, loss of reputation and loss of consumer confidence. Numerous data controllers adjusted the design of their solutions, the scope and manner of data collection, safeguards and security measures in advance, thereby avoiding the negative consequences of wrong decisions.

The Information Commissioner also issued four new guidelines and instructions for operators of unmanned aircrafts regarding the performance of impact assessments on the protection of personal data:

- Guidelines on the use of private devices for business purposes (BYOD) address the risks arising from the increasing use of private mobiles, tablets and laptops for official purposes. This raises a number of questions and risks regarding the potential loss, unauthorized access and other abuses of personal data of employees and his related persons (e.g. children and partners). On another note, private mobile devices may also store inadequately secured business data, as employees often access company's emails, applications and other corporate systems via their private devices. The Information Commissioner recommends companies and institutions planning to introduce such systems to think thoroughly about what they want and do not want to achieve by this, and gives its recommendations on how to safely and lawfully introduce mobile device management systems.
- Guidelines on the processing of personal data from the Central Population Register describe the conditions to lawfully collect and process data on individuals, when, who and for what purposes can obtain personal data from the Central Population Register (detectives, insurance companies, police, banks, municipalities, lawyers, insolvency administrators...), how personal data may be further processed, and how access to data is regulated. They also provide answers to frequently asked questions and give specific examples.
- Guidelines for managers of multiple dwellings address a number of issues that are faced by the property owners and managers of multiple dwellings, such as when can the manager demand personal data from owners and/or tenants; which personal data may owners and/or tenants acquire from other owners and/or tenants; which personal data of other owners and/or tenants may the manager disclose to third persons and organisations; and when is video surveillance of the apartment building, parking lots and entrances into individual apartments permissible.
- Guidelines for the protection of personal data in employment relationships constitute an urgent update to the materials of the Information Commissioner in the area that is filled with dilemmas raised by employers, employees and trade unions. The Guidelines explain the legal basis for collecting, processing and publishing of personal data of employees, they cover the field of occupational safety and health (e.g. the control of alcoholism and sick leave) and processing of personal data in the framework of trade union activity. A special chapter is dedicated to the issue of control over the work means (e-mail, internet, telephones, computers), which may lead to prohibited behaviour if data are used unintentionally.

In 2016, the Information Commissioner strengthened cooperation with stakeholders and thus achieving synergy and multiplier effects. Building on the existing activities in the field of awareness raising on the safe use of the Internet in cooperation with the Safe.si project, the Institute for Corporate Security Studies (ICS) and the Agency for Communication Networks and Services, the Commissioner signed a cooperation agreement with the SI-CERT, the national cyber security incident response centre. The Commissioner also entered into agreements with the Association of Banks of Slovenia and the Consumers' Association of Slovenia. The Commissioner also works closely with the Civil Aviation Agency, assisting with educating the operators of unmanned aerial vehicles and raising the awareness of privacy and personal data protection. The Commissioner carries out joint activities with partners, such as giving talks at conferences, publishing expert papers and conducting training sessions, and it thus reaches data controllers and individuals more effectively. In the coming year, the Information Commissioner will further strengthen the cooperation with stakeholders in other areas.

The Information Commissioner also devotes much attention to the accessibility of information through its website, which was renewed in 2016. The Register of personal data filing systems is available to the public in an open format, and a search engine is available for browsing through the collection of decisions and opinions, which will be further improved. In order to improve usefulness and user-friendliness of the website, the Information Commissioner conducted an external testing of the user experience and the results will be known next year.

The preventive work of the Information Commissioner is also reflected in expert cooperation in the inter-service working groups. In addition to participating in the Inspection Council, it is worth mentioning the

Commissioner's participation in the Interdisciplinary Working Group for eIDAS Regulation on Electronic Identification, cooperation in the drafting of regulations, cooperation with the Ministry of Public Administration in various digitalization projects, and participation in the Council for the development of informatics.

The Information Commissioner's experts raise awareness of the importance of privacy and personal data protection by giving talks at various conferences, professional events, consultations and round tables. In 2016, they actively participated at INFOSEK 2016, Cryptoparty 2016 and CSA CEE Cloud Security Summit and at the International Conference on Data Protection (Moscow), the 24th International Conference on Auditing, the 7th International Conference Days of Corporate Security, at the Conference on Mobile Phone Safety, at XV. Labor Law and Social Security Days. The Commissioner's experts also took part in the round table entitled The Right to Privacy and New Technologies at the Criminal Law Days, and they attended the Digital Conversion Opportunity for Slovenia and the Open Data Festival.

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 the ministries, the National Assembly, bodies of self-governing local communities, other State bodies, and holders of public powers regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations regulating personal data.

In 2016, the Information Commissioner issued more than 100 opinions on amendments to laws and draft laws. The Commissioner also noted that there is no decrease in the alarming number of new draft laws and regulations that may affect the individuals' privacy, but are adopted in expeditious procedures without proper analyses and assessments of consequences for the protection of constitutionally guaranteed right to privacy and personal data protection.

4.2 Relations with the public

Throughout 2016, 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. By organising a variety of workshops and seminars, it provided for the continuing education of liable entities and person. The employees at the Commissioner gave as many as 98 pro bono lectures. Furthermore, the Commissioner also takes an active role in the Centre for Safer Internet of Slovenia and the Web Eye, which are active in the field of safe use of the Internet. Within the framework of the latter activity, it conducted a number of lectures on the protection of personal data on the Internet for schoolchildren, teachers and parents. The Information Commissioner continued its prevention activities and dedicated a great deal of attention to disseminating tools and aids for raising awareness. In addition to the Annual Report for 2015, the Commissioner released the following guidelines: the Guidelines on the use of private devices for business purposes (BYOD), the Guidelines on the processing of personal data from the Central Population Register, the Guidelines for managers of multiple dwellings and the Guidelines for the protection of personal data in employment relationships.

The Information Commissioner marked the European Personal Data Protection Day (28 January) and organised a round table entitled What privacy protection for the new era of control? The event was dedicated to the challenges brought by drones (the unmanned aircrafts) and related technologies for control to the guardians and advocates of privacy. We should realise that the use of drones, aside from its many advantages, also brings certain risks for the security of people and the respect for basic human rights. The Information Commissioner awarded a good practice award in the field of personal data protection, which is now already an established tradition. The Ambassador of Privacy award was given out to the Institute for the development of the unmanned systems, which carries out a number of activities aimed at raising awareness among the users, the public and the experts on various aspects of the use of unmanned aircrafts and actively strive for a prudent regulation thereof. With its work, the Institute actively contributed to the implementation of the privacy-by-design concept, whereby privacy has its place in the very design of technological, regulatory or management solutions.

The International Right to Know Day (on 28 September) was dedicated to the challenges that were brought about to cultural institutions (libraries, museums and archives) by the EU Directive on the re-use of the public sector information and the national legislation (namely, the ZDIJZ-E Amendment). In cooperation with the Ministry of Public Administration and the Ministry of Culture, the Commissioner organised an event entitled "Open data – open and rich society", with the help of which it wanted to raise awareness of the impact of the use of data of the cultural institutions on the development of an open and rich society. The Information Commissioner awarded the Ambassador of Transparency award for good practice in the field of access to public information.

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. The Commissioner engages in international cooperation and in the legislative procedures of the EU as envisaged by the 95/46/EC Directive. Thus, in 2016, the Information Commissioner participated at the EU level at plenary meetings and in the work of four of the many subgroups of the Working Party established under Article 29 of the 95/46/EC Directive (The Article 29 Data Protection Working Party - WP29). In addition, the Commissioner participated in six working bodies of the EU, which oversee the implementation of personal data protection in the context of large EU information systems.

In 2016, the Information Commissioner continued to participate 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 2016, the Information Commissioner hosted representatives of similar institutions from Albania, Ukraine, Serbia and Moldova to whom it presented its activities and good practices in its fields of competence.

The Information Commissioner answered 95 questions and questionnaires from data protection authorities from abroad, international organizations, academic and research institutions and non-governmental organizations from abroad.

In 2016, the Information Commissioner actively participated in two international projects, CRISP (Evaluation and Certification Schemes for Security Products) and ARCADES (Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union). The CRISP project 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. From June 2016 to the end of the year (and until March 2017), the activities of the entire consortium were led by the Information Commissioner as the leader of the Work Package 7. The Information Commissioner considers that one of the greatest successes of managing the consortium in 2016 was an exceptionally successful workshop on certification and personal data protection aimed at data protection supervisory bodies, which the Commissioner organized with the assistance of the University of Jaume I of Castellón and the Spanish Personal Data Protection Supervisor in Madrid on 30 September 2016.

The ARCADES project is aimed at promoting the awareness of personal data and privacy protection in elementary and secondary schools. Within the framework of the project, standardized materials and tools are being prepared at the EU level, which teachers and counsellors in elementary and secondary schools will be able to use for teaching about privacy and personal data protection. In October, the Information Commissioner organised two full-day training seminars for teachers and professional pedagogues, where topics from the Handbook for Teaching Privacy and Personal Data Protection in Primary and Secondary Schools were presented. The Handbook is available in different languages and accessible to all schools in the EU. In December, a competition was held for the best lesson on the topic of privacy and personal data protection.