Information Commissioner of the Republic of Slovenia

'15 Annual report

We are pleased to present you with the Information Commissioner's report for the year 2015. The last ten years of the Commissioner's operations have brought about a significant increase in the awareness and understanding of the fields of access to public information and privacy and personal data protection both with the general and professional public. The data controllers have a relatively good knowledge of their duties and the same applies to many bodies liable for disclosing public information. Nevertheless, many violations still occur and this requires preventive and inspection activities and represent a considerable challenge for the Information Commissioner in its role as an appellate body. The Commissioner must be constantly active in raising awareness in both of its fields of competence. While the European surveys confirm that a general awareness of data protection is comparatively good in Slovenia, the rapid developments in technology cause certain misunderstandings of the right to privacy and personal data protection. By the same token, the Commissioner observes certain impermissible violations also in the field of access to public information.

In the field of access to public information, the Information Commissioner received in 2015 the largest number of complaints so far, totalling 632 cases (a year earlier, there were 578 complaints). In the appeal procedures against the rejection decisions, the Information Commissioner issued 309 decisions, which is the highest annual number since its establishment. During this process, the Information Commissioner endeavoured to resolve the complaints swiftly and with a minimum delay for the applicants. The average processing time of appeals against rejection decisions, in which a special declaratory procedure is required, was 62 days. This is within the deadline for resolving such cases prescribed by the General Administrative Procedure Act.

In the Information Commissioner's assessment, a renewed increase in the number of complaints regarding administrative silence (after the number of these complaints has been dropping in the last two years) is a negative indicator, which proves a lower responsiveness of first instance bodies. It is particularly worrisome that the majority of complaints received refer to bodies that form state administration and other bodies of the state. On the other hand, the Information Commissioner processed only 15 complaints against the decisions of entities under dominant influence, which represents less than 3% of all complaints.

In 2015, the Information Commissioner considered several important appeal cases in regards to their substance, whereby cases in the field of environmental information deserve a special mention. In this field the Commissioner also 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, and already eight such cases in 2015. This shows that the public is increasingly aware of the importance of access to environmental information, and the Information Commissioner hopes that such awareness is also spreading among the bodies. These issues also attracted 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. In 2015, there were two resounding cases; one was in relation to disclosure of environmental review of Cinkarna Celje and the other concerned the disclosure of the amended investment programme for building of a replacement block in Šoštanj Thermal Power Plant. In both cases, the Information Commissioner granted the applicants' appeals and instructed the relevant bodies to disclose the requested information. 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 2015 was also marked by the adoption of amendment ZDIJZ-E in December of this year, whereas the amendment entered into force in May 2016. The amendment brought changes especially to the field of re-use of public information, while important changes were also brought to the regime of charging the cost of access (and re-use) of public information. The Information Commissioner welcomed the legislator's decision to maintain the solution that only material costs may be charged for access to public information, and not the hourly rates of civil servants who handled such requests.

In the area of re-use of public information, the Information Commissioner dealt with only one complaint case in 2015. An exceptionally low number of complaints in this field indicates a low level of awareness of the applicants of the legal options available to them when the bodies reject their request for re-use. Nevertheless, changes in this field are expected in the future. Namely, the previously mentioned amendment ZDIJZ-E implementing in Slovenian legal order the amendment to the European Directive 2013/37/EU of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, will bring a number of novelties to this field. One of such novelties is the expansion of the scope of re-use obligations to museums, libraries and archives. The Information Commissioner expects that the number of complaints received in this field will increase in the coming years and thus the scope of his work will also increase.

In the course of implementing the inspection activities in the field of personal data protection, the Information Commissioner dealt with 791 inspection cases in 2015, of which 343 were in the public sector and 448 in the private sector. In 2014, there were a total of 628 cases. The Information Commissioner dealt with 104 minor offences procedures on the basis of the established violations (in 2014, there were 95 such procedures). The Information Commissioner received six requests for permission for the implementation of biometric measures (four were received in 2014), nine applications for permission to connect two or more filing systems (14 received in 2014) and 14 applications for authorisation for the transfer of personal data to third countries (countries outside the EU) (11 received in 2014). In 2015, the Information Commissioner received 100 complaints from individuals for having been refused access to their personal data (in 2014 there were 67 such complaints).

In 2015, the Information Commissioner dealt with 791 inspection cases in total, out of those it received 615 applications (in 2014 this number was 605) and initiated 176 cases on its own initiative. Similar to previous years, a significant number of applications concerned the implementation of video surveillance, the use of personal data for the purposes of direct marketing, the 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.

In 263 cases, the Information Commissioner, upon examining the statements in the applications, already determined that the conduct for which the application was filed did not constitute a violation of the provisions of ZVOP-1. The reasons for certain applications being unfunded can be attributed to the poor knowledge of applicants of the rules in the field of personal data protection and the competences of the Information Commissioner. In addition to that, the applicants regrettably often file applications that are impossible to satisfy in the inspection procedure of the Information Commissioner. A large number of such applications that are filed without a just cause and the statutory need for its examination hinder the performance of the so-called preventive inspection in areas where the need for such preventive actions is greater. In addition to examining the applications, the Information Commissioner also conducted the so-called planned ex officio inspections, which are carried out each year in accordance with the adopted annual plan. This includes examining judicial authorities, police, managers of multiple dwellings and private sector companies that provide video surveillance and process personal data of customers and users of their services.

When carrying out inspections, the Information Commissioner finds that violations predominantly occur due to ignorance or misunderstanding of legislation (especially in the private sector due to economic interests of offenders), but to a lesser extent also due to negligence or deliberate misconduct and violation of legislation. Persons liable who conduct their business in fictitious business premises, usually without any employees and who usually perform their business online, present one of the major problems in carrying out inspection supervision. It is basically impossible to conduct inspection procedures against such companies and the enforcement of unpaid fines is equally unsuccessful. For this reason, the Information Commissioner proposed to the two competent Ministries that they regulate this field appropriately. Namely, the current situation sets a bad example for many similar companies that will try to find ways to circumvent legal provisions in the future.

In 2015, the Information Commissioner issued more than 1660 opinions upon request from individuals and legal persons, as well as a record number of guidelines and reports on specific topical themes in the field of personal data protection. The purpose of these guidelines is to provide controllers, all in one place, with key responses to issues in thematic areas and to offer useful tools for their implementation in practice. Thus, the Commissioner issued in 2015 (new) Guidelines on the implementation of video surveillance, Guidelines on the use of GPS tracking devices, Guidelines on the recording of telephone calls, Guidelines on data processing agreements and Guidelines on the protection of personal data. Due to the fact that the data sharing agreement with the US, Safe Harbor, is no longer valid, the Commissioner has updated three of its guidelines that touch upon this area, namely: Guidelines on transferring personal data, Data protection in relation to cloud computing, and Cloud computing - a summary for small businesses. Adding to that, the Information Commissioner issued a report on the use of unmanned aerial vehicles (drones), where it examined the implications posed by the increasingly widespread use of drones on human rights with the emphasis on the right to privacy. The Commissioner gave the recommendations to the legislator, drone operators and individuals on the safe use of these vehicles.

In 2015, more than 100 public and private sector controllers and processors referred to the Information Commissioner when they drafted legislation, developed solutions or projects and encountered dilemmas

regarding personal data protection that they wanted to address appropriately before the implementation. Thus, the Information Commissioner among other things emphasised the need for necessary safeguards to achieve adequate protection of patients' privacy in developing the e-Health system, considering privacy protection in the preparation of amendments to the Prevention of Money Laundering and Terrorist Financing Act, the Financial Instruments Market Act, the revision of SISBON system and the establishment of the Single Credit Register and the amendments to the Organization and Financing of Education Act. In addition to conducting the privacy impact assessments, the Information Commissioner in 2015 also carried out numerous trainings for public sector controllers and a wide range of professionals. The purpose of such trainings is, in particular, to improve the attitude towards the protection of personal data in the preparation of rules, the introduction of systemic solutions and in the everyday dealing with personal data.

The year 2015 was also the year when the negotiations concerning the upcoming EU personal data protection regime have been completed. A consensus was reached on the reform of the legislative framework and it was embodied in the General Data Protection Regulation. With the expected final vote in 2016 and coming into force in 2018, the Regulation will bring about many changes to the field of personal data protection. More emphasis will be given to data protection officers, data protection impact assessment and privacy by design, certification. The Regulation foresees stricter penalties and broadens its scope to cover foreign controllers that provide their services to European citizens. The Regulation will require numerous additional measures for the effective implementation in practice, and thus the government in 2016 faces significant challenges in this field.

Many people wonder whether the battle for privacy has already been lost. So many people publicly share volumes of information about themselves and their close ones on the Internet, we hear about massive and ubiquitous eavesdropping and the air is frequented by unmanned vehicles that enable the invasions in our spatial, communication and information privacy. The Information Commissioner acknowledges that protecting privacy in the information society is extremely difficult and it therefore devotes a lot of attention to balancing rights and to raising awareness in order to show that privacy is not about hiding something bad, but about having the power to make decision about oneself (i.e. the informational self-determination). Even though a lot of work has already been done, we, the guardians of privacy, are at the beginning of our work, as large scale processing of personal data is in its infancy. The digitisation of homes, cities and transport infrastructure will result in large amounts of personal data to be processed. The introduction of concepts such as big data and the Internet of Things represents tremendous challenges for data protection, which will require constant monitoring and development of new tools for the protection of human rights.

The year 2015 was a success, but we face many challenges in the year that follows. We will only be able to see the results of our work if individuals, controllers and all other persons liable are aware of the importance of both fundamental and constitutionally guaranteed human rights, the right to access to public information and the right to personal data protection. We also need to ensure and demand from everyone that these two rights are respected to the fullest extent possible. Facing many different societal challenges, it will be the implementation of these two rights that will have a crucial impact on the quality of individuals' lives, as they are important indicators of how truly democratic a society is.

Mojca Prelesnik,
Information Commissioner

1 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

The Information Commissioner performs its statutory tasks and competences in two fields:
1. In the field of access to public information;
2. 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] (hereinafter 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 (hereinafter 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 planned - 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 Paragraph 4 of Article 9 and Paragraph 3 of Article 10 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 (Article 48 of the ZVOP-1), 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, the provisions of Article 45 of the ZMed and 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),
- 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),
- Banking Act[9] (exercising supervision with regard to the collection and processing of personal data in the SISBON system),
- Electronic Communications Act[10] (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; the provisions on retention of traffic and location data which are acquired or processed in relation to the provision of public communications networks or services and disclosure of such data to competent bodies),
- Consumer Credit Act[11] (supervision of creditors with regard to obtaining data on consumers' creditworthiness and indebtedness).

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 2015, the Information Commissioner had 36 employees, five of which were temporary staff. Compared to 2014, the number of employees 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 2015, the budget was set at EUR 1,315,579.14, of which EUR 1,070,572.16 were spent for wages and salaries and EUR 126,686.61 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 38,472.27 for investment (e.g. purchase of office equipment, hardware and telecommunications equipment).

[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. 99/2010 - official consolidated text 5, with amendments; hereinafter ZBan-1.
[10]Official Gazette of the Republic of Slovenia, no. 109/2012, as amended; hereinafter ZEKom-1.
[11]Official Gazette of the Republic of Slovenia, no. 59/2010, as amended; hereinafter ZPotK-1.

Commissioner. In the beginning of 2015, the budget was set at EUR 1,315,579.14, of which EUR 1,070,572.16 were spent for wages and salaries and EUR 126,686.61 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 38,472.27 for investment (e.g. purchase of office equipment, hardware and telecommunications equipment).

Due to the budgetary constraints and austerity measures adopted by the Slovenian Government in 2015, 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 governs 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 implements 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. 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.

At the end of 2015, amendment ZDIJZ-E[16] was adopted, introducing 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 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. The Government of the Republic of Slovenia has already adopted a new Decree, 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.

ZDIJZ provides the right to access information that has already been created and exist 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 the bodies liable are usually 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 the so-called new bodies 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 information; 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.

The body can refuse access to the requested information if the request relates to one of the exceptions specified in the Paragraph 1 of Article 6 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). Without prejudice to the provisions of the Paragraph 1 of Article 6 of the ZDIJZ, the 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 that is considered an exception to free access, referred to in Article 6 of the ZDIJZ, this cannot be the reason for the body 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 21 of the Decree on the provision and re-use of public information,[17] 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.

[17]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 2015, the Information Commissioner received 632 appeals, of which 318 were against the refusal decisions and 314 were against the non-responsiveness of the first instance bodies (the so-called administrative silence).

In appeal proceedings against decisions in which responsible authorities refused requests for access to or re-use of public information, the Information Commissioner conducted 15 procedures against the "new" bodies, i.e. legal entities under the dominant influence of the State, self-governing local communities and other public entities. The Commissioner issued 309 decisions, five applicants withdrew their appeals, in two cases the Information Commissioner dismissed the appeals on procedural grounds, and it merged two cases into one.

In proceedings against the administrative silence, the Information Commissioner first called on the bodies 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 decided on the request of the applicant and provided the requested information to the applicants. After the body 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 17 cases, the Information Commissioner dismissed the appeal on procedural grounds due to premature or incomplete applications, eight individuals withdrew their appeals because they received the requested information, and in two cases the Information Commissioner advised the applicants that it was not competent to consider their applications and transferred their cases to a competent authorities for consideration.

In the process of handling appeals, it is sometimes necessary to review the information without the presence of the party, requesting access to public information, i.e. in camera inspection, through which the Information Commissioner identifies the state of the documents with the body. In 2015, there were 59 such inspections.

In 2015, the Information Commissioner received 251 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 competent institutions. 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 2015, 37 administrative disputes were issued against decisions of the Information Commissioner (i.e. against 11.9% of all decisions issued). Compared to the year before, when it was 10.1%, the proportion of initiated disputes slightly increased, although it declined steadily before 2014. In 2011, disputes were initiated against 13.1% of Commissioner's decisions. In 2012, the proportion was 10.5% and in 2013 8.1%. Nevertheless, the number of disputes against the Commissioner's decisions is 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 authorities and the applicants.

In 2015, the Administrative Court issued 34 judgements regarding decisions of the Information Commissioner in which it decided to:

- Uphold the application, annul the decision in part or in its entirety and refer the matter to the Information Commissioner for reconsideration (16 cases);
- Dismiss the application as unfounded (9 cases);
- Dismiss the application on procedural grounds (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 (2 cases);

- Uphold the application, annul the Commissioner's and first instance body's decision and refer the matter to the latter for reconsideration (1 case).

In 2015, the Information Commissioner did not file any requests for revision against the ruling of the Administrative Court with the Supreme Court. However, one such request for revision was filed by one of the bodies along with a request for an interim order. The Supreme Court upheld the request for the interim order and decided to withhold execution of the Commissioner's decision until the decision on the revision has been reached. The Supreme Court ruled on two requests for revision; a request for revision submitted by the Information Commissioner was dismissed on procedural grounds, so was another request for revision, submitted by one of the bodies together with a request for an interim order.

2.4 Statistics by individual fields of the ZDIJZ

Compared to previous years, the number of decisions issued in the field of access to public information increased again. In 2011, the Information Commissioner issued 251 decisions, in 2012 256 decisions, in 2013 258 decisions, in 2014 288 decisions, and in 2015 as many as 309.

The Information Commissioner issued the following decisions:
- In 125 cases it refused the appeal;
- In 103 cases it granted partial access to information;
- In 44 cases it granted the appeal in favour of the applicant;
- In 30 cases it returned the matter to the first-instance authority for reconsideration;
- In 4 cases the first instance decision was declared null;
- In 3 cases it dismissed the appeal on procedural grounds.

In its decisions, the Information Commissioner made substantive rulings with consideration of the following:
- 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 (110);
- Whether the body actually possessed the document or the public information requested by the applicant (95);
- Whether the applicant requested information or data deemed to be a business secret in accordance with the law governing companies (52);
- Whether a violation of procedural rules occurred (41);
- 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 (39);
- Whether the information requested relates to the work and personal data of civil servants and officials (29);
- Whether the public interest in disclosure outweighs the public interest or the interest of other persons in restricting access to the information requested (25);
- Whether the information originates from the field of work of the authority (19);
- Whether the authority correctly charged the fees for providing public information (17);
- Whether the requested information is protected by copyright legislation (15);
- Whether the applicant abused his/her rights under the ZDIJZ (15);
- 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 (14);
- Whether the information requested pertains to data classified in accordance with legislation regulating classified information (12);
- 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 (10);
- Whether the body violated a substantive law (10);
- 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 (10);
- The issue of a decision in procedures in which the applicant requested documents related to public procurement procedures (10);

- Whether the body to whom the request for access to public information was addressed to is in fact liable under the Paragraph 1 of Article 1 of the ZDIJZ (9);
- Whether the document requested meets the conditions for it to be deemed public information as provided for in the Paragraph 1 of Article 4 of the ZDIJZ (8);
- Whether the case concerns environmental information (8);
- 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 (8);
- 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 (5);
- 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 (4);
- Whether the information relates to the issue of confidentiality of a source (4).
- Whether the case concerns the re-use of public information (1);
- Whether the case concerns the proactive publication of information (1);
- 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 (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 (156 cases), from which ministries, constituent bodies and administrative units (111 cases), and courts, Supreme State Prosecutor and State Attorney's Office (24 cases),
- Public funds, public institutes, agencies, public service contractors, bodies exercising public powers and other public entities (106 cases),
- Local government authorities (32 cases),
- New bodies liable (business entities subject to dominant influence of public entities (14 cases)

One appeal concerned a legal entity of the private sector, but the Commissioner established that it was not liable under the ZDIJZ.

202 appeals were submitted by natural persons, 59 by private sector legal entities, 37 by journalists, and 11 by public entities.

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

In 2015, the Commissioner did not introduce any minor offenses proceedings for violation of the ZMed and ZInfP provisions.

2.6 Most significant decisions of the Information Commissioner in different areas

We present some of the most complex and interesting decisions from 2015, sorted by areas.

2.6.1. Costs

By the decision No. 090-277/2014 of 14 January 2015, the Information Commissioner annulled the decision by the Ministry of Education, Science and Sport (the body) on the costs, as the body unjustifiably charged for the consultation of the requested documentation. Namely, the body charged for the disclosure of information the cost of work at the hourly rate of civil servants who prepared the materials (i.e. the costs of searching and preparing materials). In the Commissioner's opinion, the body had no legal basis for such charging.

In the appeal procedure, the Information Commissioner found that the body did not correctly apply the transitional provision of the ZDIJZ-C, namely its Article 27. This provision stipulates that the Government

shall accept rules for charging and a uniform bill of costs referred to in Article 35 of this Act within five months from the entry into force of this Act. Until that time, the provisions from Articles 34 and 35 of the ZDIJZ shall apply. Considering the fact that the Government of the Republic of Slovenia had not yet accepted the uniform bill of costs referred to in Article 35 of the ZDIJZ-C, the provisions related to the charging of costs that were in force before the entry into force of the ZDIJZ-C, namely the provisions of the ZDIJZ, still apply. However, it is clear from the text of Paragraph 1 of Article 34 of the ZDIJZ that access to the consultation of the requested information is free of charge. In the particular case, the body should not charge the costs for consultation of the requested documents. Namely, according to the ZDIJZ and the Decree on the provision and re-use of public information,[18] the bodies may only charge for the costs if the applicant requests a copy, a photocopy or an electronic record of the required information. This is also clear from the Paragraph 2 of Article 34 of the ZDIJZ.

2.6.2 Internal functioning of the body

By decision No. 090-176/2015 of 27 July 2015, the Information Commissioner upheld the applicant's appeal and ordered the Ministry of Agriculture, Forestry and Food (the body) to disclose to the applicant all comments on the draft Management of State Forests Act, received in the course of public consultation. The body was obliged to redact personal data of natural persons.

The body refused the applicant's request relying on the exception of internal operation from Point 11, Paragraph 1 of Article 6 of the ZDIJZ. The body claimed that the disclosure of the requested information would cause disturbances in operations or activities of the body. The persons did not send the body the requested documents with the intention of publishing it publicly, but with the intention that the body takes their comments into consideration when preparing the draft law.

In the appeal procedure, the Information Commissioner examined the cited exception of internal operations of the body. The provision of Point 11, Paragraph 1 of Article 6 of the ZDIJZ provides that two criteria must be met: the information must be drawn up in connection with internal operations or activities of the body, and the disclosure of such information would cause disturbances in operations or activities of the body (specific damage test). During the procedure, the Information Commissioner found that the requested documents contain views, opinions and comments on the draft law. The authors of the documents were legal and natural persons who were not a part of the body's internal structure and they expressed their own opinions, not the opinion of the body. The documents therefore do not originate from within the body and in no way concern the internal logistics of the body or the body's opinion on the draft law. The Commissioner therefore established that the information that does not constitute internal communication or the functioning of the body, but it relates to external factors. The Commissioner also emphasized that the requested documents were sent to the body in the process of public consultation, which cannot be part of the internal process of the body by its very nature. Public consultation presents an open platform, aimed at sharing different ideas in order to increase the democracy and quality of legislation. With regard to the first criterion of the exception of internal operations, it is therefore essential that the information deriving from the requested documents do not in any way reveal the internal operations of the body. The Information Commissioner therefore concluded that the exception claimed was not provided. Nevertheless, the Information Commissioner examined ex officio whether the requested documents contain any other exceptions from free access to public information. It found that the documents include personal data of natural persons, which represent an exception under Point 3, Paragraph 1 of Article 6. The Commissioner found no legal basis for the disclosure of such personal data, so it refused the application in this part and allowed the applicant partial access to the requested documents.

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

2.6.3 Protection of personal data and civil servants

In a number of appeal procedures (decisions No. 090-112/2015, 090-120/2015, 090-133/2015 and 090-137/2015), the Information Commissioner decided on whether the information on payments made by the faculties (public institutions) on the basis of copyright contracts and work contracts are public. It granted the appeals of several journalists and ordered the Faculty of Economics in Ljubljana and the Faculty of Administration to disclose more than 4,800 contracts for copyright contracts, contracts for services and work contracts, which the faculties concluded with professors, employed at these faculties, in the period from 1 January 2005 to 10 March 2015.

When refusing the access, the faculties relied on the exception of personal data protection and on the fact that the requested information did not originate from performing public service, but from the so-called commercial part of faculties' operations. Therefore, they claimed that the information is not of a public nature.

Upon reviewing the requested contracts, the Information Commissioner found that they refer to activities related to performing of public service in higher education. These activities included, for example, performing lectures in part-time studies, part-time postgraduate studies and distance learning, performing lectures at seminars and training courses, preparation of learning materials, textbooks and other study materials, research work, preparation of study programs, writing reports for teaching authorizations, assessing the appropriateness of the doctoral dissertation topic and the submitted dissertations, performing lectures and seminars in full-time undergraduate studies, workshops, examinations, mentoring and co-mentoring, reviewing undergraduate theses, membership in commissions, execution and reviewing of exams, expert opinions on behalf of the faculty, etc.). The requested information also includes information related to employment relationship of civil servants, which is not protected information. Deciding on this case, the Information Commissioner took into consideration the fact that the Higher Education Act (ZVis)[19] clearly states that it is permitted to conclude contracts for copyrighted work for the performance of pedagogical activity only if all the possibilities for concluding employment contract have been previously exhausted and it is imperative to ensure a smooth implementation of pedagogical activities. Only in such cases may the higher education institution conclude a work contract, and even so, such a contract should not cover more than one third of the statutory prescribed pedagogical obligations and may only be concluded for a period of maximum ten months in an academic year. According to the Information Commissioner, the public has the right to know whether the statutory conditions for the conclusion of these contracts have been met, and thus the disclosure of the requested information is also in the public interest.

In addition, the Information Commissioner emphasized that the mere fact that a particular activity is not financed directly from the budget does not mean that this activity is not considered a public service. The funding of both faculties is regulated by the ZVis, which stipulates that higher education institutions are financed directly from the budget and from other sources when performing public service. In the particular case, the requested information originates from the field of work of the two faculties as they relate to the performance of public law tasks or regulated by public law rules. Thus, they represent the information of public nature under Article 4 of the ZDIJZ in their entirety. Regarding the issue of personal data protection, the Information Commissioner established that the contracts were concluded with public officials and that the information also relates to the use of public funds. Consequently, the information on the name of the individual with whom the contract was concluded, the amount received and the purpose of the payment is not protected information.

[19] Official Gazette of the Republic of Slovenia, no. 32 / 2012- official consolidated text 7, with amendments; hereinafter ZVis.

2.6.4 Protection of court proceedings

By decision No. 090-289/2014 of 24 February 2015, the Information Commissioner accepted the views of the Municipality of Maribor (the body) and the third-party participant that the requested information (a lawsuit) constitutes an exception pursuant to Point 8, Paragraph 1 of Article 6 of the ZDIJZ. The particular litigation procedure was still pending and the harm test proved there would be damage to the court proceedings if the document was to be released.

The applicant requested the lawsuit that the company Iskra d.d. lodged against the Municipality of Maribor and concerned the issue of traffic radars. The body refused the applicant's request, referring to the exception from Point 8, Paragraph 1 of Article 6 of the ZDIJZ (protection of court proceedings), as the court proceedings were still ongoing. The body was of the opinion that the disclosure of the requested document would cause harm to the court proceedings, because gathering the evidence in the proceedings must be carried out without prejudice and without influence on the views of the participants in proceedings. All hearings should be carried out, witnesses should be heard, and evidence should be produced. The body was convinced that the disclosure of documents could have an influence on the final positions of the participants in proceedings.

In the appeal procedure, the Information Commissioner verified with the competent court in what is the status of the civil procedure at hand. The court explained that the procedure was currently suspended, namely that a decision to suspend the civil procedure was issued and the litigants were referred to a mediation proceeding that has not been finished. Since the Information Commissioner found that the civil proceedings in question are still pending, it concluded that the first condition of the exception from Point 8, Paragraph 1 of Article 6 of the ZDIJZ was fulfilled. Regarding the second condition of the said exception (the harm test), the Information Commissioner accepted the views of the body and of the third-party participant. Nevertheless, due to the principle of substantive truth, the Commissioner also conducted the harm test itself. The Commissioner found that the legal proceedings have not been completed yet; that it was currently in the phase of mediation which relies on the principle of confidentiality of the proceedings; and that the court has not yet assessed each piece of the evidence (whereas the allegations in the application constitute only a part of the evidence). In view of the above, the Information Commissioner assessed that the disclosure of the requested document at this stage of the proceedings could cause such harm to the continuation of the proceedings, that the potential harm outweighs the public's right to receive the requested information. Finally, it follows from Articles 7 and 8 of the Contentious Civil Procedure Act[20] that the decision on which facts will be deemed proven, shall be based upon the opinion of the court taken after a careful and thorough evaluation of every piece of evidence in itself, and of the evidence as a whole, and considering the outcome of the entire proceedings. Thus, the court reveals no sooner than in the reasoning of the judgment, which facts it deemed proven and which unproven, for what reasons has the court taken such a view and which evidence has been taken into account. Therefore, the Commissioner took the view that before resolving the dispute, either in the context of mediation or with a judgment, it is nearly impossible to ascertain with certainty which documents are important and which are not in relation to further proceedings. Consequently, it is also impossible to predict what consequences could public disclosure have on the proceedings. A document can have no worth in one stage of the process, but may become one of the main evidence in the course of the proceedings. The Information Commissioner assessed that damage to the process would be caused if the public gained access to the content of the requested document in this stage of the process. For example, the disclosure could influence witness statements and general security of evidence in the proceedings. In case the mediation proved unsuccessful, the presiding judge would have to decide which procedural acts need to be carried out before the decision is reached. Disclosing a document before the hearing, before all documents are submitted and before all evidence are examined, would thus cause the proceedings to be carried out with more difficulty, because individual actions in the proceedings would be influenced.

In the present case, the Information Commissioner estimated that the disclosure of the requested document (lawsuit) would prejudice the implementation of the proceedings, and it therefore rejected the applicant's appeal in its entirety.

[20]Official Gazette of the Republic of Slovenia, no. 73/2007 - official consolidated text 3, with amendments.

2.6.5 Classified information

By decision No. 090-233/2015 of 15 October 2015, the Information Commissioner ordered the Judicial Council (the body) to provide data on the name, surname and percentage of confirmed cases for all local, district and higher court judges in the Republic of Slovenia for the year 2014.

The body rejected the applicant's request, referring to the exception from Point 1, Paragraph 1 of Article 6 of the ZDIJZ (classified information). The body noted that Article 78 of the Courts Act (ZS)[21] specifies that the required information is classified as "confidential". The body submitted that the ZS may prescribe confidentiality of the data in terms of Point 1, Paragraph 1 of Article 6 of the ZDIJZ, in addition to what is prescribed under the Classified Information Act (ZTP).[22]

The Information Commissioner did not agree with the body's explanation the ZS may prescribe confidentiality of the data in terms of Point 1, Paragraph 1 of Article 6 of the ZDIJZ for the judiciary. The legislator made it clear in the course of adopting the ZDIJZ that the exception from Point 1, Paragraph 1 of Article 6 of the ZDIJZ refers to the classified information in terms of the ZTP. Such an explanation is suggested by the grammatical legal explanation itself, because the exception from Point 1, Paragraph 1 of Article 6 of the ZDIJZ refers to a law that governs classified information and not the laws that govern classified information. In the view of the Information Commissioner, the ZS does not introduce a special regime of protection of classified information, but protects certain personal data of the judges and prevents general access to such information and the possibility of abuse. The ZTP governs the issue of determination, protection and access to information in a unified, comprehensive manner and same for all state bodies, as this is the only way to prevent the abuse of the institute of "classified information". Thus, there is no logical explanation and it was not the intention of the legislator for the ZS to create a "new type of classified information" what would be absolutely secret, would not be bound by the criteria set up in the ZTP, and would at the same time fall under the exceptions established by the ZDIJZ. Thus, the Commissioner could not follow the body's explanations. One of such obvious examples of personnel information that would be deemed classified in accordance with the body's interpretation of Paragraph 3 of Article 78 of the ZS, is the name of a judge. However, such information, as settled in the caselaw and being related to exercising of a public function, is considered public information and is even published online. It would make no sense that the same information would be considered as classified and at the same time would be published. This even strengthens the view that the aim of the provisions of the ZS is to protect personal data of the judges and not to protect classified information. The Commissioner agrees with the body that Paragraph 3 of Article 79 of the ZS provides for the permissible purposes of processing of personal data from personnel files and the manner of handling of such data. But the provisions are aimed at regulating the purposes of collecting and further processing personal data, not classified information. The Information Commissioner also noted that the data were not marked as classified; that there is no authorized person within the organization that had marked the information as classified; and that no assessment of the possible adverse effects of the disclosure was made. Thus, the Information Commissioner concluded that the requested documents do not meet the criteria for the exemption outlined in Point 1, Paragraph 1 of Article 6 of the ZDIJZ. In addition, the content of the requested documents does not fall under any of the fields of regulation, established in Article 5 of the ZTP. In the case at hand, the exception of classified data in accordance with Point 1, Paragraph 1 of Article 6 of the ZDIJZ does not apply.

[21]Official Gazette of the Republic of Slovenia, no. 94/2007 - official consolidated text 4, with amendments; hereinafter ZS.
[22]Official Gazette of the Republic of Slovenia, no. 50/2006 - official consolidated text 2, with amendments; hereinafter ZTP.

2.6.6 Environmental information

By decision No. 090-108/2015 of 14 July 2015, the Information Commissioner ordered the Ministry of the Environment and Spatial Planning (the body) to disclose to the applicant the report on the environmental review of Cinkarna Celje.

The body rejected the applicant's request, stating that Cinkarna Celje did not give its consent to the disclosure of the report. Cinkarna Celje, as third party participant, claimed that the requested document constituted an exception from Point 2, Paragraph 1 of Article 6, of the ZDIJZ, namely that it is its business secret, based on the decision that the company adopted.

The Information Commissioner did not need to determine whether the exception of business secret applies, because the requested report concerned the environmental impacts assessment, aimed at determining the level of contamination of soil and groundwater on the land that is managed by the third party participant. In such cases the provision of Point 2, Paragraph 1 of Article 6 needs to be taken into account. This provision stipulates that, regardless of the exceptions to free access, access to information is permitted if the information relates to environmental emissions, waste, dangerous substances in factory or information contained in safety report and other information if so determined by the act regulating the environment protection. Due to the provisions of the Aarhus Convention, exceptions from free access in relation to environmental information are not absolute. The fact that environmental information should be public is confirmed by Article 13 of the Environmental Protection Act[23] (ZVO-1), which refers to the Aarhus Convention and the ZDIJZ as regards access to environmental data. All of the above mentioned legal instruments stipulate publicity of data relating to emissions, waste, dangerous substances in factory and safety report and other information if so determined by the ZVO-1.

The Information Commissioner emphasized that a statutory presumption applies to environmental information, namely that the disclosure of such information is always in the prevailing public interest. In addition, the ZGD-1, which regulates business secrets, stipulates that information that are public in accordance with a law or information on violations of the law or good business practices cannot be determined as business secrets.

The Information Commissioner granted the applicant's appeal and ordered the body to disclose the requested environmental report.

[23]Official Gazette of the Republic of Slovenia. no. 39/2006 - official consolidated text 1, with amendments and supplements; hereinafter ZVO-1.

2.6.7 Classified information

By decision No. 090-163/2015 of 15 July 2015, the Information Commissioner ordered the Ministry of Foreign Affairs (the body) to disclose to the applicant certain parts of the Report on the internal control at the Embassy of the Republic of Slovenia in Paris.

The said Report was created on the basis of the regular internal control of the Embassy of the Republic of Slovenia in Paris in accordance with the Foreign Affairs Act.[24] It was marked with an "internal" level of classification and there was a written assessment of the possible adverse effects signed by the chief diplomatic supervisor. The internal control verified whether the Embassy's entire operations had been conducted in a proper manner, economically and lawfully.

The Information Commissioner noted that the content of the Report cannot be easily categorized as falling in the field of foreign affairs within the meaning of the Classified Information Act (ZTP) simply because the Embassy is a foreign "unit" and a part of the body that exercises the powers in the field of foreign affairs. The report is comparable to similar (e.g. audit) reports on the operation and performance of state administration bodies and the wider public administration. Such reports are freely accessible public information.

The Information Commissioner further noted that the content of the Report does not relate to economic and financial matters important in the process of implementing foreign policy and for relations with other countries. The Report relates only to the general, internal financial-material functioning of the Embassy, and is not directly related to conducting foreign affairs. The content of the Report describes only general operation and functioning of the Embassy (e.g. in terms of its financial documentation, business payment cards, representation expenses, business travel (travel forms, costs ...), company vehicle, transport to work and costs of food, health insurance of public employees, company phones ...). Therefore, disclosing the Report could not cause adverse effects for the security of the State and for its political or economic benefits.

The Information Commissioner also drew attention to the fact that certain acts of the Embassy and/or of its employees may fall under a definition of criminal offense of abuse of authority, embezzlement, fraud, damage to public funds or misappropriation. Such information in the Report may be classified due to the provision of Article 6 of the ZTP, which states that information that has been defined as classified in order to cover up a criminal offence, the exceeding or abuse of authority, or some other unlawful act or behaviour shall not be considered classified.

The Information Commissioner however followed the argumentation of the body that certain parts of the Report relate to systems, devices, projects and plans relevant to foreign affairs, namely data on security equipment, deficiencies in video surveillance systems, the location of video surveillance systems, the alarm system, password security systems, etc. According to Paragraph 5 of Article 5 of the ZTP, this information may be classified, insofar as the disclosure to the unauthorised person would cause or would obviously cause adverse effects to the security of the country or to its political or economic interests. Thus, parts of the Report were justifiably and correctly classified with the "internal" level of classification.

The Information Commissioner partly granted the applicant's appeal and ordered the body to allow the applicant partial access to the requested Report.

[24] Official Gazette of the Republic of Slovenia, no. 113/2003 - officially consolidated text 1, with amendments; hereinafter: the ZZZ-1.

2.6.8 Internal functioning of the body

By decision No. 090-141/2015 of 22 October 2015, the Information Commissioner ordered the Real Estate Fund of the Pension and Disability Insurance (the body) to allow the applicant the consultation of the Legal Opinion on the compliance of charging for the rent in terms of legislation and concluded rental agreements.

The body rejected the applicant's request with the argumentation that the requested documents do not fall under the definition of public information pursuant to Article 4.a of the ZDIJZ and that the body is not liable to provide information pursuant to Paragraph 1 of Article 1 of the ZDIJZ since it does not qualify as a public fund.

The Information Commissioner had to first determine whether the body is liable to disclose public information as a business entity under the dominant influence of public law entities (Article 1.a of the ZDIJZ) or whether it is liable to disclose information as a legal person of public law or a public service provider (Article 1 of the ZDIJZ). It was noted that the body is registered in the Register of bodies liable for public information in accordance with Article 1 and Article 1.a of the ZDIJZ. The ZDIJZ establishes a statutory presumption (which can be rebutted) that the legal entity registered in the Register is a body liable under the ZDIJZ. The body challenged this presumption so the Information Commissioner assessed whether the body is a body liable in accordance with Article 1 of the ZDIJZ, namely, whether it is an entity of public law.

The Information Commissioner found that the body was established under the Pension and Disability Insurance Act,[25] and not by a contract. Establishing an entity by a contract is a typical way of establishing companies, that is, persons of private law, which are establishes as a result of the free economic initiative. The tasks of the body are also determined by the law in order to pursue goals of a public nature and to exercise public functions. The entity was established with the purpose of managing real estate and providing assigned rental apartments and service residence for the pensioners and other elderly persons. Furthermore, the Information Commissioner found that the basic capital of the body was provided from public funds - from the funds of the Pension and Disability Insurance Institute (the Institute). In addition to the fact that the body manages public funds when exercising its statutory activities, the body is also subject to supervision by the Court of Audit of the Republic of Slovenia.

The Information Commissioner thus established that according to all of the above mentioned criteria, the body is a body governed by public law and, as such, liable under Article 1 of the ZDIJZ in the entire sphere of its activity.

Nevertheless, the requested document meets all the criteria to be categorized as copyright work (as a presentation of scientific, educational or technical nature). In such cases, the ZDIJZ allows only for the consultation of the document. As a result, the Information Commissioner partially granted the applicant's appeal and ordered the body to allow him to consult the requested opinion.

[25]Official Gazette of the Republic of Slovenia, no. 106/1999, with amendments; hereinafter ZPIZ-1.

2.6.9 Business entity under dominant influence; business secret

By decision No. 0902-17/2014 of 30 January 2015, the Information Commissioner instructed Telekom Slovenije (the entity liable) to provide the applicant with the documents that represent legal transactions that qualify as sponsorship and donation agreement. The applicant requested the information relating to journalists, media outlets or legal entities governed by public law, where civil servants are employed.

The body liable refused the applicant's request on the grounds it did not conclude any sponsorship or donation agreements and that it is not a business subject under the dominant influence of public law entities. The body liable also disputed its potential obligation to disclose information that had been created prior to the entry into force of the ZDIJZ-C.

The Information Commissioner found that the body liable is registered in the Register of bodies liable for public information as a company under direct or indirect majority ownership by entities of public law. Namely, the Republic of Slovenia owns, directly or indirectly, a 74.27% stake of the capital of the entity liable (source: AJPES). Throughout the entire period that covered the applicant's request, legal entities of public law owned a "majority share of the subscribed capital". However, it is not essential in this case whether these shares are entitled to voting rights, as claimed by the body liable. The body liable is obliged to disclose public information created during the entire period under the dominant influence, irrespective of the fact whether the information was created before or after the entry into force of the ZDIJZ-C, that is, before 17 April 2014.

The Information Commissioner then assessed whether the requested documents meet the essential characteristics of a sponsorship agreement. These characteristics are: 1) the expected mutual benefit; 2) the sponsor's intention of promoting or enforcing its name, company, trademark, image, its activities, products or carrying out marketing analysis (test marketing) and 3) the sponsoree can help the sponsor to achieve its aim with a counterpart. The following characteristics, however, are not essential to define sponsorship: formality; designation; who or what is a sponsoree; type and form of the sponsor's contribution; type, form and nature of the sponsoree's counterpart; the actual effect of the sponsor's contribution and of the sponsoree's counterpart; the actual fulfilment of the agreement; the irreversibility of the sponsor's contribution; the term used by the general public.

In this particular case, the requested documents represent the forms for the internal procurement of goods, printed procurement orders, lease agreements, etc. and by their effect represent sponsorship (test) or donation (gift) legal agreements or they at least have the same effects as sponsorship or donation agreements. These agreements relate to journalists, media outlets or legal entities governed by public law, where civil servants are employed. The Information Commissioner determined so by consulting the Media register, the Register of independent journalists and the Business register, while in some cases this information originated from the documents themselves. In addition, the requested documents originated in the period when the entity liable was under the dominant influence of the entities of public law, the entity liable had the documents at its disposal. Thus, the requested documents represent information of a public nature.

Considering the fact that the body liable relied on the exception from Point 2, Paragraph 1 of Article 6 of the ZDIJZ (business secret), the Information Commissioner also found in the appeals procedure that all requested documents were visibly and clearly marked with a stamp "business secret". Such documents therefore meet the so-called subjective criterion for determining business secrets. However, the Information Commissioner found that the body liable cannot classify certain information as business secret in accordance with the provision of Paragraph 3 of Article 39 of the Companies Act (ZGD-1), which determines that information that are public according to the law cannot be designated as business secret. These are information on the type of the transaction, the contractual partner, the contractual value, and the date and duration of the transaction. In accordance with Paragraph 1 of Article 6.a of the ZDIJZ, these data constitute absolute public information, which should thus be made available to the applicant in the specific case. Therefore, the Information Commissioner partly granted the applicant's appeal.

2.6.10 The body's field of work

By decision No. 090-33/2015 of 8 July 2015, the Information Commissioner rejected the applicant's appeal on the count that the Waldorf School in Ljubljana (the body) did not dispose of the requested information. The Waldorf School is only liable to provide information in part of its activities that present the performance of the public service. In the rest of its activities it is not liable to provide information.

The Information Commissioner found that the body is a legal entity of private law. It is a private school, founded by natural persons. Nevertheless, the school is a public service provider, as it implements publicly recognized education programmes, which means that it is a body liable under Article 1 of the ZDIJZ. The field of work of the public service provider within the meaning of Article 4 of the ZDIJZ is defined by the public service they perform. In so far as the body also carries out a commercial activity, it is not liable under the regime of access to public information in the "commercial" part of its activities.

The body receives assigned public funds from the state and municipality budgets in order to implement publicly recognized education programmes. However, it is not, as a person of private law, obliged to keep separated records on spending public funds and on spending funds earned in the market.

The Information Commissioner found that it is not possible to grant the applicant's request for documents relating to the entire analytical gross balance sheet broken down by individual items and to the customers and suppliers records. On the one hand, the Information Commissioner found that the body is not obliged to keep two separate accounts (for public and for market funds) and on the other hand, that the body is not obligated to create the documents and do analyses especially for the purpose of meeting the applicant's request. The remaining documents that the body does possess relate to information on the body's commercial activities which the body is not obliged to provide. As mentioned, such documents do not fall within the body's field of work as they are not related to the performance of the public service and consequently do not constitute public information. Therefore, the Commissioner could not grant the applicant's appeal.

2.6.11 Internal functioning of the body; personal data

By decision No. 090-241/2015 of 24 November 2015, the Information Commissioner ordered the University of Ljubljana (the body) to provide the applicant with two documents. One was a report drawn up as a result of an internal audit at the Faculty of Administration in 2009 and the other was a response report from the said Faculty, with redacted personal data that need to be protected.

The body rejected the applicant's request referring to Point 11, Paragraph 1 of Article 6 of the ZDIJZ (internal functioning of the body). It claimed that disclosing the documents would cause disturbances to the internal functioning of the body or its activities, because the publication of the said documents would result in a number of journalistic inquiries. Furthermore, the body claimed that the internal audit and consequently the audit report were an integral part of the system of internal control of public finances. The body must ensure independence of internal auditors, who must not be under any influence or under the influence of the public, which might influence their independent functioning. By disclosing the internal audit reports, the institution of internal audit, which is aimed particularly at the management of the body, would lose its meaning.

The Commissioner did not follow these arguments. In the appeal procedure, it found that the requested document was created in connection with the internal functioning of the body. Nevertheless, the body failed to demonstrate the damage that would be caused by disclosing the requested report. The body did not specify clearly the damage to the internal functioning of the body and it only stated that the disclosure would result in a number of journalistic enquiries, while it should be noted that the body has its own public relations service, which is trained exactly for these sorts of challenges. The Information Commissioner also took the view that the disclosure of the requested documents cannot have an effect on the independence of the auditors, since all audit procedures have already been completed. Therefore, both elements of the exception under Point 11, Paragraph 1 of Article 6 of the ZDIJZ are not cumulatively fulfilled, which means that this exception does not apply.

However, the Information Commissioner found that the documents contain some personal data that need to be redacted, namely the names and surnames of students, candidates and civil servants in connection with their voluntary supplementary insurance and the names and surnames of contact persons other than

public servants. Furthermore, the Information Commissioner found that the name, surname and signature of the state auditor, of the Faculty of Administration employees and other civil servants (professors from other faculties and University employees) are related to the execution of public functions or employment relationship of the civil servant. For this reason, the disclosure of this information is permissible as these personal data are not protected by the law.

2.6.12 Public procurement

By decision No. 090-148/2015 of 27 May 2015, the Information Commissioner granted the journalist's appeal and ordered Mariborski vodovod, d. d. (the body) to disclose the requested documents. The applicant requested the documents that demonstrate legal bases (tender, the process of collecting the bids, received bids and concluded contracts) in connection with the transactions, concluded between the Municipality of Maribor, the body and three companies in the period from April 2013 to December 2014, when Andrej Fištravec was the Mayor.

The Information Commissioner first found that all public procurement contracts relate to the management of public water supply facilities and equipment (namely, the construction work at the pumping station, the replacement of the water supply pipeline, the transfer and reduction of the pressure in the water supply network). Thus, there is no doubt that the requested information fall within the scope of implementation of public services, which is within the competence of the body. Therefore, the information fall within the scope of definition of public information in accordance with Article 4 of the ZDIJZ.

One of the third party interveners invoked the business secret exception under Point 2, Paragraph 1 of Article 6 of the ZDIJZ. The Commissioner consulted the requested bid and found that it is correctly marked as a business secret in its entirety, as it was accompanied by the company's decision designating the entire bid as a business secret, except the parts where the existing legislation establishes publicity of information. The Commissioner thus assessed whether the data from the credit rating system S.BON AJPES can be considered a business secret, as they were designated as such by the third party intervener, or they are considered public in accordance with the law and they cannot be designated as business secret as per Paragraph 3 of Article 39 of the ZGD-1.

The Commissioner noted that the third party intervener is obliged to submit to AJPES in accordance with Article 58 of the ZGD-1 its income statements and balance sheet. The AJPES publishes annual reports, consisting of at least the balance sheet and the income statement, on its website, which is available to anyone on the basis of free registration. The Commissioner found that the credit assessment S.BON AJPES includes detailed information on the company's business credit rating that only the company may receive for itself. Thus, the third party intervener (the company) can designate such information as its business secret and therefore the body is not obliged to disclose it.

With regard to all other documentation that was the subject of the applicant's request, the Information Commissioner found that they represent freely accessible public information that the body is required to provide to the applicant.

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

In 2015, the Information Commissioner received the highest number of complaints thus far in the field of access to public information, totalling 632 cases (in 2014, there were 578 complaints). It received 303 appeals against the rejection decisions (320 in the previous year), 314 complaints against the administrative silence (258 the year before) and 15 appeals against the written refusal answers from business entities under dominant influence. The Information Commissioner received 251 requests for an opinion or clarification from applicants and bodies liable. In total, the Commissioner handled 883 matters. Compared to the year 2014, the number of complaints against rejection decisions decreased, while the number of complaints against administrative silence has yet again increased. In the appeal proceedings against the rejection decisions, the Information Commissioner issued 309 decisions, the highest number since its establishment. The Information Commissioner strived for a swift handling of the appeals with a minimum delay for the applicants. The average time to decide upon an appeal against a rejection decision, in which a special declaratory procedure was required, was 62 days. This is within the timeline for resolving such cases prescribed by the General Administrative Procedure Act.

According to the Information Commissioner's assessment, a renewed increase in the number of complaints against the administrative silence (after the number of these complaints has been dropping in previous two years) is a negative indicator, which proves a lower responsiveness of first instance bodies. It is particularly worrisome that the majority of complaints received refer to bodies that form State administration and other bodies of the State. On the other hand, the Information Commissioner processed only 15 complaints against the decisions of entities under dominant influence, which represents less than 3% of all complaints. It can be deducted from this that with regard to the new entities liable the situation "stabilized" in practice after the entry into force of the Amendment ZDIJZ-C. It follows from the appeal proceedings data that this law does not put excessive burdens on the business entities under dominant influence. Nevertheless, the majority of these appeals end up before the Administrative Court of the Republic of Slovenia, as the business entities under dominant influence lodge administrative disputes against the Information Commissioner's decisions more frequently than other bodies liable. In this period, the Administrative Court of the Republic of Slovenia decided in two significant cases answering the question which information is a business entity under dominant influence obliged to transmit to the public. In these two cases the Court upheld the Commissioner's view that basic data from contracts for a copyright work, consulting and sponsor contracts is freely accessible public information. However, a request for a review has been filed in both cases, which means they continue before the Supreme Court of the Republic of Slovenia, which has not delivered its decisions as of yet.

The Information Commissioner also estimates that the increase in the number of complaints regarding administrative silence dictates that more effort is put in training the bodies liable in how to apply the law in practice. Therefore, in 2015, the Information Commissioner once again paid much of its attention to the education of bodies liable. The "pedagogical" mission of the Information Commissioner is same as the mission of any other appellate body; it advises the bodies liable and the applicants, taking into account its competencies and the impartiality principle. On the other hand, the Information Commissioner notes that the applicants are well-informed of their right to access public information and practice it often. This is due to the fact that the process of accessing public information is simple for the applicants, without costs (as there are no administrative fees) and relatively fast. This is also reflected in the fact that the majority of applicants for public information are individuals, that is, "lay" natural persons.

In 2015, the Information Commissioner considered several important appeal cases in regard to their substance, whereby the cases related to access to environmental information deserve a special mention. In this field the Commissioner also 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, and in 2015, there were already eight such cases. This shows that the public is increasingly aware of the importance of access to environmental information, and the Information Commissioner hopes that such awareness is also spreading among the bodies. These issues also 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. In 2015, there were two resounding cases; one was in relation to disclosure of environmental review of Cinkarna Celje and the other concerned the disclosure of the amended investment programme for building of a replacement block in Šoštanj Thermal Power Plant. In both cases, the Information Commissioner granted the applicants' appeals and instructed

the relevant bodies to disclose the requested information. Slovenian legislation sets the highest standards of transparency for environmental information and allows basically no legal exceptions when it comes to publicity of such information.

The year 2015 was also marked by the adoption of the Amendment ZDIJZ-E in December of this year, whereas the Amendment entered into force in May 2016. The Amendment brought changes especially to the field of re-use of public information, while important changes were also brought to the regime of charging the cost of access (and re-use) of public information. The Information Commissioner welcomed the legislator's decision to maintain the solution that only material costs may be charged for access to public information, and not the hourly rates of civil servants who handled such requests. The Information Commissioner has been drawing attention to this problem ever since 2009; the main problem derives from the regulations. The Commissioner therefore hopes that the Government will soon adopt a new regulation, implementing a uniform bill of costs in accordance with Article 35 of the ZDIJZ and thus abolish the individual bills of costs that enable the charging od labour costs. The hope is that this will happen as soon as possible, and in any case before the entry into force of the ZDIJZ-E, which will enter into force on 8 May 2016.

In the area of re-use of public information, the Information Commissioner dealt with only one complaint case in 2015. An exceptionally low number of complaints in this field indicates a low level of awareness of the applicants of the legal options available to them when bodies reject their request for the re-use. The field of re-use of public information has a significant economic potential, but in practice this potential remains underutilized. Nevertheless, changes in this field are expected in the future. Namely, the previously mentioned Amendment ZDIJZ-E implementing in Slovenian legal order the amendment to the European Directive 2013/37/EU of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, will bring a number of novelties to this field. One of such novelties is the expansion of the scope of re-use obligations to museums, libraries and archives. The Information Commissioner expects that the number of complaints received in this field will increase in the coming years and thus the scope of its work will also increase.

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[26] 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)[27] 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 a 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 2015 conducted a total of 791 inspection cases of suspected violations of the act, which is more than in previous years (628 in 2014, 712 in 2013). 343 of those cases concerned suspected violations in the public and 448 in the private sector. Most of the inspections were initiated upon receiving a complaint (615 in total, of which 189 in the public and 426 in the private sector), while the rest were initiated ex officio (176 in total, of which 154 in the public and 22 in the private sector) and in accordance with the annual inspection plan.

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

- Unlawful disclosure of personal data – 208,
- Establishing of the catalogues of filing systems and supplying them to the Information Commissioner for the inclusion in the Register of filing systems – 138,
- Unlawful collection or requiring of personal data – 125,
- Abuse of personal data for direct marketing purposes – 120,
- Unlawful video surveillance – 59,
- Inadequate security of personal data – 39,
- Processing of personal data contrary to the purpose for which they were collected – 34,
- Cookies – 18,
- Miscellaneous: processing of personal data on contractual basis; 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, the transfer of personal data to third countries; and monitoring the implementation of the provisions of the ZVOP-1 as a whole by the Information Commissioner in ex officio inspection procedures – 50.

Within the framework of the above inspection procedures, 106 on-site inspections were carried out in total; 37 in the public and 69 in the private sector. Additionally, 64 inspections of websites were carried out, mostly in relation to the oversight of the provisions on cookies. In order to address the established irregularities, the Information Commissioner issued a total of 44 warnings on the record (11 in the public and 33 in the private sector), 12 regulatory decisions (3 in the public and 9 in the private sector) and 42 preliminary decisions (5 in the public and 37 in the private sector). In addition and in accordance with the principle of procedural economy and the need to conduct proceedings fast, the Commissioner issued 175 written or oral warnings of the irregularities, which the persons liable implemented in full.

[26]Official Gazette of the Republic of Slovenia, no. 86/2004; hereinafter ZVOP-1.
[27]Official Gazette of the Republic of Slovenia, no. 67/2007; hereinafter ZVOP-1A.
[28]If it is established that personal data have been processed unlawfully, the Information Commissioner must, prior to issuing the decision by which it orders the cessation of illegal processing, notify the person liable in accordance with the principle of the right to be heard. In this notification, the Information Commissioner states its reasons for believing there is no legal basis for the processing of personal data, together with the arguments in favour of this view. Namely, according to the case law and the adversarial principle, the person liable must have the opportunity to acquaint himself with the views of the Information Commissioner prior to the issuing of the regulatory decision. In practice, this means that after acquainting themselves with the views of the Commissioner, the majority of persons liable cease to process personal data unlawfully and there is no more need for the regulatory decision to be issued.

Due to violations of the provisions of the ZVOP-1, 104 minor offence proceedings were initiated in 2015 (95 in 2014 and 106 in 2013), of which 56 were against legal persons from the public sector and their responsible persons and 15 were against legal entities in the public sector and their responsible persons. 33 proceedings were against individuals.

In minor offence proceedings, including those initiated in previous years, the Information Commissioner issued 8 warnings and rendered 61 minor offence decisions (28 cautions and 33 fines). Furthermore, the Information Commissioner issued 66 additional warnings for minor violations (18 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 eight requests for judicial protection. The highest number of violations concerned the issue of unlawful processing of personal data (48), unlawful video surveillance (28), inadequate security of personal data (25), infringement of direct marketing provisions (21), unlawful purpose of collecting and further processing of personal data (14), and irregularities with regard to the establishment of catalogues of filing system and supplying them to the Information Commissioner for the inclusion in the Register of filing systems (10).

In 2015, the Information Commissioner received a total of 12 decisions of the local courts on requests for judicial review pertaining to this and past year's decisions. In five of those cases the court reduced the imposed fine, in five it dismissed the request for judicial review as unfunded and in seven the court annulled the Commissioner's decision and closed the minor offence proceedings.

The Information Commissioner issued 1,667 written opinions or referrals to opinions already issued. In addition, the State supervisors answered 1,702 questions over the telephone (every working day between 9 am and 3.30 pm there is a State supervisor on duty at the office). This means that, all together, the Information Commissioner advised more than 3,300 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, the Internet, education, video and audio surveillance, access to personal data, insurance, security of personal data, health data).

In 2015, the Information Commissioner received six applications (in 2014 there were four and in 2013 there were 11) for issuing the decision on permissibility of implementing biometric measures. The Commissioner issued three decisions, in two cases it granted the request for the implementation of biometric measures, and rejected one application:

- The Information Commissioner granted the request for the introduction of biometric measures on employees for the purposes of performing the activities of the applicant (the production, integration and testing of biometric systems, or the production and development of access control systems, which functions also on the basis of recognizing biometric characteristics). The Commissioner allowed biometric measures in order for the applicant to be able to test his devices acting on the basis of fingerprint identification, face or voice recognition of an individual. When deciding upon the request, the Information Commissioner took into account that employee attendance data, supplied from the testing of biometric devices and systems, are in fact not real data and that the use of biometrics for the purposes of testing is voluntary.
- The Information Commissioner granted the request for the introduction of biometric measures on employees for the purposes of protecting the property using two fingerprint readers. The employees subject to these measures would be those individuals that are authorized to enter the vaults - cash registers, located at the applicant's premises and containing a relatively large amount of cash. When deciding upon the request, the Information Commissioner took into account the potential material damage that could be caused to the applicant in case of theft of high-valued property and that the measures would only be implemented over a narrow circle of employees.
- The Information Commissioner rejected the applicant's request for the implementation of biometric measures with a fingerprint reader for the purposes of keeping employees' attendance records with the aim of fraud prevention. The Information Commissioner found that the introduction of biometric measures for registering employees' attendance was not strictly necessary for performing the applicant's activities and for the protection of business secrets. Introducing such measures would mean excessive and unnecessary interference with privacy of individuals, because it would suffice to introduce contactless cards or other comparable measures (e.g. personal passwords) or combinations thereof in order to achieve the goal of keeping the attendance records.

The Information Commissioner received 14 applications in 2015 (in 2014 it received 11 and in 2013 14) for the transfer of personal data to third countries. It issued seven decisions allowing the applicants (namely the trade and service companies, telecommunications providers, a company marketing pharmaceutical products) to transfer employee data, data of business partners, customers and users of services to third countries (for example to India, Malaysia, the Philippines, China, the USA, Bosnia and Herzegovina, Serbia). The allowed purposes for the transfer were: providing support and maintaining information technology services, marketing and marketing communications and providing a common human resources system. All cases concerned the transfer of personal data to data processors (data importers) who will process personal data on behalf of data controllers (data exporters). The data importers and exporters opted for the standard contractual clauses model and both annexes to Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries in accordance with the Directive 95/46/EC which provides for adequate safeguards for the protection of privacy and the fundamental rights and freedoms of individuals.

The Information Commissioner set aside its the decision from the year 2010, which established that the United States provides an adequate level of protection of personal data in so far as it relates to transfer of personal data to organizations operating in accordance with the Safe Harbor principles. The Commissioner took this decision as a result[29] of the decision No. C-362/14 of 6 October 2015 of the EU Court of Justice in the case of Maximillian Schrems vs. Data Protection Commissioner. The EU Court of Justice annulled the Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles. This annulment means that these principles no longer provide an adequate level of protection of personal data that are transferred from the Community to organizations established in the United States.

[29]When deciding on the appropriate level of protection of personal data in third countries, the Information Commissioner is bound by the decisions of the competent EU body.

In 2015, the Information Commissioner received nine applications (14 in 2014 and six in 2013) to connect personal data filing systems. The Commissioner issued twelve decisions granting a direct computer connection (whereas the connecting code was either the personal identification number or the tax number) of the following personal data filing systems:

1. The Register of consents for the single permit and the Register of notices referred to in Paragraph 2 of Article 33 of the Employment, Self-employment and Work of Foreigners Act (Employment Service of Slovenia) with the Register of Aliens (Ministry of the Interior)
2. Data filing systems kept in the framework of the KURIR Information System (Ministry of Labour, Family, Social Affairs and Equal Opportunities) with:
   - the central database of rights deriving from public funds and personal data filing systems kept in the Information system for the social work centres (Ministry of Labour, Family, Social Affairs and Equal Opportunities);
   - Record of taxes (Ministry of Finance, Financial Administration of the Republic of Slovenia),
   - The Register on remuneration payments kept in the framework of the Register of the insured persons and pension beneficiaries from the pension and disability insurance (Pension and Disability Insurance Institute of Slovenia),
   - The Central Population Register (Ministry of Internal Affairs and Public Administration).
3. The list of individuals performing personal complementary work (the Agency of the Republic of Slovenia for Public Legal Records and Related Services) with the Central Population Register (Ministry of the Interior), Record of the insured persons and users of rights from the compulsory pension and disability insurance, and the Register of the insured persons (Pension and Disability Insurance Institute of Slovenia) with the Register of unemployed persons, the Register of persons that are temporarily unemployable, the Register of persons included in the active employment policy programmes, the Register of job seekers, the Register of Aliens (Employment Service of Slovenia),
4. The e-INS Information System and the e-Enforcement Information System (the Supreme Court of the RS) with the Register of liquidators (Ministry of Justice),
5. The Tax register (Ministry of Finance, Financial Administration of the Republic of Slovenia) with the Register of cases in insolvency proceedings (Supreme Court of the RS),
6. The Register of insured persons and users of rights from compulsory pension and disability insurance (Pension and Disability Insurance Institute of Slovenia) with the Computerized database on rights for parental protection and family benefits - ISCSD-SN (Ministry of Labour, Family, Social Affairs and Equal Opportunities),
7. The Tax Register (Ministry of Finance, Financial Administration of the Republic of Slovenia) with the List of individuals performing personal complementary work (Agency of the Republic of Slovenia for Public Legal Records and Related Services),
8. The Central register of participants of education and Register of students and graduates (Ministry of Education, Science and Sport) with the Register of beneficiaries of subsidized food (Student Organization of Slovenia),
9. The Register of the insured persons and users of rights from the compulsory pension and disability insurance (Pension and Disability Insurance Institute of Slovenia) with the Register of natural persons performing the activity of generating electricity and the List of individuals performing personal complementary work (Agency of the Republic of Slovenia for Public Legal Records and Related Services),
10. The Register of entities (Ministry of Agriculture, Forestry and Food) with the Register of insured persons and the Register of persons liable (Pension and Disability Insurance Institute of Slovenia),
11. The Register of members of civil protection, civil servants in the field of civil protection and disaster relief and citizens who volunteer to participate in the performance of civil protection, disaster relief and aid; the Register of candidates for contractual civil protection and contractual members of civil protection; the Register of persons involved in assessing the risks, planning and implementing the civil protection, disaster relief and aid, residents living in at-risk areas, in apartment and other buildings, and involved in public services, institutions and organizations whose activities are important for the civil protection, disaster relief and aid and damage assessment after an accident; the Register of members of bodies active in the field of protection against natural and other disasters; the Register of persons who have passed professional exams in the field of civil protection and disaster relief; the Register of victims of natural or other disasters (Ministry of Defence of the Republic of Slovenia, Administration of the Republic of Slovenia for Civil Protection and Disaster Relief) with the Central Population Register (Ministry of the Interior).

In 2015, the Information Commissioner received 100 appeals in relation to the right to access to 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 67 such complaints 2014 and 68 in 2013). 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 16 such complaints (five in 2014 and 11 in 2013). After examining the appeals, the Commissioner found that comparing to previous years, the number of administrative silence cases, that are cases when data controllers do not respond to the individuals' requests for access to personal data, decreased. In 2015, the share of such cases decreased to 33% (in 2014 the share was 49% and in 2013 52 %). The appeals lodged in 32 cases concerned State bodies (mostly ministries and bodies affiliated to ministries), 18 appeals concerned healthcare institutions, seven cases involved educational institutions and banks respectively, while the rest of the complaints concerned various data controllers (such as societies, insurance companies, centres for social work, telecommunications operators). In 33 cases, data controllers reacted immediately to the Information Commissioner's call to grant the individuals' the right to consult and obtain the requested information or to provide them with the explanation as to why they will refuse this right. The Information Commissioner issued eight decisions whereby it partially granted the individuals' complaints and ordered the data controllers to enable individuals the right to access their personal data. Seven 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 12 rejection decisions and dismissed two 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 26 individuals on how to proceed in their case and referred five complaints to the competent authorities.

The Information Commissioner also dealt with two complaints concerning the right to supplement, correct, block, erase and object:

1. The individual asked the Information Commissioner to immediately cease disclosing his personal data to the persons liable who were, are or will be supervised by the Commissioner's data protection inspectors. The applicant complained to the Information Commissioner that the inspector revealed the source of the report to the person liable and thus violated the provision of Article 16 of the Inspection Act[30] due to unlawful disclosure of personal data. The request alleged that the violation occurred when the inspector served the person liable with the decision rejecting the applicant's request for being included in the inspection procedure as a third party intervener. The Information Commissioner rejected the request, because the applicant's request to be allowed participation in the procedure and the decision refusing such participation cannot be considered as a report which the Information Commissioner is obliged to protect in accordance with the provision of Article 16 of the ZIN (the secrecy of the sources of a report). Pursuant to Article 142 of the General Administrative Procedure Act[31] and in accordance with the principle of examination of parties and adversarial principle, the Information Commissioner must immediately notify other interested parties of the procedure (in the specific case, the person liable) of the request to be allowed participation in the procedure. The interested parties have the right to object to the participation of another person in the procedure and thereby exercise their procedural rights.
2. The Information Commissioner received a complaint regarding the administrative silence of the data controller. The controller failed to respond to the applicants' objection and request pursuant to Article 32 of the ZVOP-1 in a timely manner. The applicants requested that the controller immediately deletes all the videos containing their personal data, collected by means of video surveillance at certain locations. In addition, they demanded that the controller immediately ceases to conduct video surveillance at the specific locations. The Information Commissioner rejected the applicants' request as unfounded, because it had already conducted the inspection procedure with regards to this specific video surveillance and it had concluded that the video surveillance conducted by the data controller – the person liable in this procedure does not violate the provisions of the ZVOP-1. The video surveillance is conducted for legitimate purposes - the protection of property, which has been intentionally damaged several times in the past. The video surveillance system is appropriately marked and in addition to that, the individuals cannot expect a particularly high level of privacy in an open public space. The applicants challenged the Commissioner's decision before the Administrative Court of the Republic of Slovenia.

In 2015, the Information Commissioner did not file any requests for a review of the constitutionality, nor did it receive any judgments of the Constitutional Court of the Republic of Slovenia in relation to the requests already filed.

[30]Official Gazette of the Republic of Slovenia, no. 47/2007-UPB1 and 40/2014, hereinafter: ZIN.

3.2 Selected cases involving a violation of personal data protection

3.2.1 Collection of personal data for the purposes of direct marketing on the basis of customer recommendations

The Information Commissioner initiated an inspection procedure after receiving several reports and reading about the suspected unlawful processing (collection) of personal data on different websites. In the course of the inspection procedure, the Commissioner found that the person liable collected personal data of potential clients for the purposes of conducting free testing of cosmetic products. The collection of personal data was conducted, among others, in a way that a client, visiting the cosmetic salon, filled in a form with personal data of third persons that the client wanted to recommended free testing of products. The personal data on the form included the name and surname, telephone number, age, employment status and the "comment" section for the entry of data on, for example, kinship, relationship with the person being recommended, the hours for contacting the person). The key data for the person liable was the telephone number, which was used to conduct the direct marketing.

The Information Commissioner found that no legal basis for the processing of personal data of third parties, laid down by Article 10 of the ZVOP-1, existed. Possible legal bases for the private sector are: statute, consent of the individual, conclusion and fulfilment of the contract, necessity to exercise the legitimate interests of the person liable. In addition, the Commissioner established that personal data in the recommendation form for the purposes of direct marketing had not been collected in accordance with Paragraph 1 of Article 72 of the ZVOP-1, as they were not obtained from publicly accessible sources or within the framework of the lawful performance of activities. Pursuant to Paragraph 2 of Article 72 of the ZVOP-1, only personal name, address, telephone number, e-mail address and fax number may be used for direct marketing purposes. Other personal data may only be used on the basis of individuals' consent. Thus, the data controller violated the said provision by collecting information on the age and employment of individuals.

For all the reasons stated above, the Information Commissioner ordered the person liable to cease with the collection of personal data of third persons for the purposes of inviting them to a free treatment. The exception from this rule is, of course, if the data controller's client, who gave the personal data, clearly states and demonstrates that the third person had given him a prior consent for transmitting certain personal data to the data controller for the purposes of direct marketing. In addition, the controller must destroy all personal data on individuals that it had collected unlawfully. The person liable carried out all of the imposed measures.

3.2.2 Video surveillance in public areas

The Information Commissioner initiated an inspection procedure on the suspicion of unlawful implementation of video surveillance in public areas. The Commissioner found that the person liable conducted permanent video surveillance of almost the entire public area of the central square along with the surrounding buildings. The data controller explained that the purpose of implementing such video surveillance is to ensure the protection of people and property owned by the local community. In the area there are all vital institutions (e.g. the bank and the post office) as well as a defibrillator, which is owned by the local community. In addition, video surveillance cameras contribute to more order and peace and people's sense of security. This position was proven with the increase in the number of unrests that supposedly occurred when the cameras were temporarily out of order.

The ZVOP-1 (or any other statute) does not explicitly regulate video surveillance of public areas. Thus, the Information Commissioner assessed whether all the conditions from Paragraph 4 of Article 9 of the ZVOP-1 have been met cumulatively for the video surveillance of the public square to be regarded lawful. The said provision of the ZVOP-1 provides that in the public sector, personal data may be exceptionally processed if this is necessary for the exercise of lawful competences, duties or obligations of the public sector, provided that such processing does not interfere with the legitimate interest of the data subject. The Commissioner, however, found that the person liable did not only perform video surveillance over the public areas or the protected property (for example, over the exposed defibrillator or other movable or immovable property owned by the municipality). The video surveillance was implemented in far greater and disproportionate extent over the property that was not owned by the municipality (e.g. it recorded entrances and windows of

the surrounding buildings on the square that were privately owned). With such measures, the data controller infringed the right to privacy of individuals - either the residents of the square who were under permanent (video) surveillance, or every-day visitors and passers-by. With regard to the use of video surveillance system for ensuring public order and peace, the Information Commissioner explained that specialised bodies, in particular the Police, were in charge of providing such services. Using the "public order and peace" as an excuse could justify all-encompassing video surveillance of public areas.

The Information Commissioner concluded that video surveillance over the entire square is unlawful. The data controller is potentially entitled to conduct video surveillance directly over the defibrillator owned by it and installed on the facade of the post office on the square for the purposes of protecting property and also ensuring safety of people, as the defibrillator is specifically designed to protect health and safety of the people. The Commissioner thus ordered the municipality to cease with the video surveillance over the entire square and to erase irreversibly all recordings of this video surveillance system. The person liable executed the Commissioner's decision by directing the camera, which previously recorded the entire square, exclusively on the defibrillator.

3.2.3 Inadequate security of personal data in a web application

The Information Commissioner initiated an inspection procedure upon receiving a report, which stated, that the person liable published in the Supervisor application personal data of individuals, namely of the members of a particular company, which has never done any business as it has never issued any invoices. The Commissioner verified the statements made in the report by entering certain search terms in the Google search engine. By doing so, the Commissioner noticed that the search engine allows searching through the Supervisor using the name and surname of shareholders as a search term and that in this way the company and the shareholders' data are accessible notwithstanding the fact that the company was deleted from the Business register in 2013.

The Information Commissioner found that the person liable only published personal data in the Supervisor application which, in accordance with the Court Register of Legal Entities Act (ZSReg),[32] were accessible through the AJPES website. However, in accordance with the provisions of Paragraph 5 of Article 7 of the ZSReg, the method of search enabled by the person liable in the application Supervizor, is prohibited. At the moment when the person liable imported data from the Court register, obtained from AJPES, into the Supervisor, it should have provided for the same data protection and disclosure regime as is guaranteed by AJPES. Namely, searching for personal data on the AJPES website and via Google Search Engine and similar web search engines is not possible in a manner that would allow to put in the search engine only the name and surname of the founder, shareholder, member of the supervisory board, etc. However, the person liable failed to implement such measures. Due to inadequate security of personal data, the data controller made it possible for the internet users to obtain information on whether a particular person is a founder, a shareholder, a representative or a member of the supervisory board in a particular entity (and which entity) by simply entering the name and surname of the person in the web search engine. This was made possible despite the clear provision of the ZSReg, which states that searching for personal data is permissible only if entering the combination of the name and personal identification number, tax number or the address of the residence. The person liable failed to prevent search engines to allow searches by name and surname, which could be done, for example, by excluding the specific subpages from being searchable by using the so-called robots.txt files, or by displaying these data in a form that is not easily machine-readable (for example, as an image).

In view of the above, the Information Commissioner ordered the data controller to protect personal data of the representatives, the members of the supervisory authorities, the shareholders and the founders of business entities on the Supervisor application, which is available on the controller's website. The protection should be achieved by means of preventing the tools of the search engines, such as Google, to access individuals' names and surnames. The aim of such protective measures is to ensure that the Internet users will not be able to access information on where (in which business entities) a specific person (with a name and surname) is a representative, a member of the supervisory board, a shareholder or a founder. The person liable executed the Commissioner's decision and updated and upgraded the Supervisor application in the course of the inspection procedure so as to include only accurate and up-to-date information.

[32]Official Gazette of the Republic of Slovenia, no. 54/2007, as amended; hereinafter ZSReg.

3.2.4 Unlawful collection of personal data of ticket holders

The Information Commissioner concluded an inspection procedure which was initiated on the basis of a report which stated that the person liable, without the individuals' knowledge, collects and processes personal data of holders of train subscription tickets, namely the data on which trains they took, the day and the hour of the travel and the travel route.

In the course of the inspection procedure, the Commissioner found that the person liable offers several types of tickets to passengers. The data controller collects data on particular trips only from the passengers who use of contactless chip tickets (the chip holds the information on the ticket holder and the ticket), whereas these tickets are issued to holders of subscription tickets and for certain types of ticket for railway workers and holders of discounted tickets. Location data (day and time of the travel, route and the number of the train boarded by a particular passenger) were recorded in the database when the train conductor read the chip with a mobile terminal and thus checked the ticket validity.

The Information Commissioner assessed whether there is any legal basis in accordance with Article 10 of the ZVOP-1, which establishes various legal bases for the processing of personal data in the private sector. The Commissioner noted that the collection of location data is not foreseen by any law, nor did the person liable obtain individuals' consent. The ticket holders were not even aware of the fact that the data controller will, in addition to data that the individuals provide when purchasing the ticket, process (collect and keep) details of their trips. The Commissioner took a view that despite the fact that the passenger and the person liable enter into a contractual relationship when the passenger purchases a ticket (a transport contract), processing of location data is not necessary for the fulfilment of such a contract. By purchasing the subscription ticket, the traveller receives the right to an unlimited number of trips throughout the entire territory of Slovenia or on a certain route during the period of validity of the ticket. If a passenger possesses a ticket for an unlimited number of journeys on all routes, it is therefore irrelevant on which route he is travelling. If the passenger has a ticket for a specific route, it is only important that he enters the train on a route that has been paid. The temporal and geographical validity of the ticket can be verified by the conductor based on the data on the chip, namely the data about the ticket holder (his name, surname and ticket information), ticket type, validity period, route, type and class of the train. For this reason, it is not necessary to store such personal data in any special data filing system. In the course of the inspection procedure, the person liable also failed to demonstrate that processing of location data is necessary for performing the obligations under the contract that it concluded with the state for the implementation of the obligatory public utility service of passenger rail transport (e.g. for reporting on the quality of services, statistical purposes).

Since the Information Commissioner concluded that there is no legal basis for processing of location data in the statute or in the individuals' consent, the Commissioner ordered the data controller to cease collecting the said personal data of the subscription tickets' holders and to delete their personal data from all data carriers. The person liable executed the specified measures.

3.2.5 Collection and publication of personal information in the Supervisor application

The Information Commissioner conducted an inspection procedure with the aim of assessing the lawfulness of processing (extraction and further processing and, in particular, publication) of personal data in the Supervisor application. This application was available on the website of the person liable. Following the content of the reports, that the Information Commissioner received in this case, the Commissioner focused the inspection procedure on the processing of personal data of those individuals that received payments from public sector entities on the basis of copyright and/or work contracts (hereinafter referred to as recipients).

It was established in the procedure that the person liable established a special data filing system in 2011 when it began receiving data from the Public Payments Administration (PPA) on the payment transactions to and from the budget users' sub-accounts. This special data filing system was named "Database on budget users' payment transactions" (the PTPU database) and was updated on a daily basis and contained personal data of recipients of funds (e.g. the name and surname, the paying entity, the amount, date, currency and the purpose of payment, the bank account number). Despite the fact that the person liable had a legal basis for acquiring personal data necessary for performing its statutory functions in the provision of Article 16 of the Integrity and Prevention of Corruption Act (ZIntPK),[33] the Information Commissioner found that acquiring information on bank account numbers of recipients from 2011 up to 4 March 2015 from the PPA was unlawful. This is because the first statutory task that the person liable performed which justified the acquisition of personal data was when it initiated a systemic investigation on 4 March 2015. Considering the statutory retention period for the data processed by the PPA (which is 10 years), the person liable could obtain data on payment transactions of recipients only from 4 March 2005. However, the Commissioner found that the person liable acquired data from 1 January 2003 onwards. Therefore, the Information Commissioner warned the person liable that it is not allowed to publish the recipients' data relating to payments which are older than 4 March 2005, which the person liable took into account and adjusted the application.

Regarding the publication of personal data, the Information Commissioner concluded that information relating to payments made by public sector entities to the recipients of funds based on copyright or work contracts (name and surname of the recipient, purpose, amount and date of payment) are public information in accordance with Paragraph 3 of Article 6 of the ZDIJZ, as they are information on the use of public funds. The Commissioner found that, by publishing data of recipients in the Supervisor application, the data controller pursued a legitimate purpose of ensuring transparency of the public sector operation, referred to in Article 75 of the ZIntPK. In addition, the body also took into account the principle of proportionality with regard to publishing data, as the body, during the inspection procedure, limited the time of publication and set the amount above which the information on funds received is to be published. Namely, the body publishes only data of recipients who received, in total, over a period of ten years, more than 150,000 EUR. This represents only a good one percent of all recipients of funds.

Since there was a suspicion that the person liable received data of other individuals from the PPA unlawfully as well (i.e. not only data of the recipients), the Information Commissioner initiated another inspection procedure against the controller.

The Information Commissioner found that since 2011, the person liable systematically and regularly obtained data from the PPA on bank account numbers of all individuals who were payers or recipients in the payment transactions of budget users since 2001. The controller included these data in its database (the PTPU database) and only some of these data were further processed for the purposes of specific procedures. Article 16 of the ZIntPK clearly sets out the conditions under which the controller is allowed to obtain data (a reasoned request, necessity of receiving data in order to perform a specific statutory task). Thus, the Information Commissioner concluded that the mentioned Article can by no means be understood as a general authorization for the unlimited collection of protected personal data and for the creation of a new data filing system, which is not provided for by any law and in which the controller stocks data which it may, one day, need in one of its procedures for which it is competent. As described above, the controller, as one of the State bodies, unlawfully interfered with the right to personal data protection of a large number of individuals. In vast majority, these individuals could not even be investigated by the person liable and could not be subjects of any other procedure under its jurisdiction according to the mere provisions of the ZIntPK. Accordingly, the Information Commissioner ordered the controller to irrevocably delete all those bank account numbers from the PTPU database whose holders are natural persons, except the bank account numbers of the recipients of payments made on the basis of copyright and work contracts. The person liable

[33] Official Gazette of the Republic of Slovenia, no. 69/2011 - official consolidated text 2; hereinafter ZIntPK.

executed the Commissioner's decision.

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

In 2015, the Information Commissioner in relation to the implementation of inspection supervision in the field of personal data protection, handled:

- 791 inspection cases, of which 343 were in the public sector and 448 in the private sector (628 cases in 2014, 712 cases in 2013, 725 cases in 2012, 682 cases in 2011 and 599 cases in 2010); and
- 104 minor offence procedures (95 cases in 2014, 106 cases in 2013, 158 cases in 2012, 136 cases in 2011 and 179 cases in 2010).

In addition to inspection and minor offence procedures, the Information Commissioner received and handled in the year 2015:

- 1,667 requests to issue a written explanation or an opinion in relation to specific questions (2,040 in 2014, 2,460 in 2013, 2,191 in 2012, 2,143 in 2011, and 1,859 in 2010);
- Nine requests for a decision on the permissibility of connecting data filing systems (14 in 2014, 6 in 2013, 9 in 2012, 14 in 2011, and 9 in 2010);
- Six requests for a decision on the permissibility of implementing biometric measures (4 in 2014, 11 in 2013 and 2012, respectively, 9 in 2011, and 6 in 2010);
- 14 requests for authorisation of transfer of personal data to third countries (11 in 2014, 14 in 2013, 5 in 2012, 4 in 2011 and 8 in 2010); and
- 100 appeals regarding the right to access to data subject's personal data (67 in 2014, 68 in 2013, 63 in 2012, and 85 in 2011 and 2010, respectively).

Of the 791 inspection cases that the Information Commissioner handled in 2015, 615 were initiated on the basis of a report, and 176 were initiated on the Commissioner's initiative. In the public sector sphere,198 reports and complaints were filed and in the sphere of the private sector 465. Similarly as in previous years, there were many reports on the use of personal data for the purposes of direct marketing, on publication of personal data on websites, on implementation of video surveillance systems, on redirecting and consequently reading of e-mails received by employees on their company's e-mail address, and on inadequate security of personal data.

It should be noted that in 2015, the Information Commissioner found in 263 out of 663 examined reports that it is possible to conclude from the statements in the report alone, that the reported conduct does not constitute a breach of the provisions of the ZVOP-1. Therefore, as many as 40% of reports were unfounded. The reason for a relatively high number of unsubstantiated reports is that the applicants lack the knowledge of the regulatory framework 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.

In addition to handling the reports, the Information Commissioner also carried out the so-called planned ex officio inspections on the basis of an adopted annual plan. In 2015, the planned inspections over the compliance with the provisions of the ZVOP-1 focused on judicial authorities, the police, managers of multiple dwellings and private sector companies that provide video surveillance and process personal data of customers and users of their services.

Statistical data on the performance of inspection supervision show that the number of regulatory inspection decisions issued by the Information Commissioner has significantly decreased compared to previous years. On the one hand, this is due to the fact that only minor irregularities are detected in the inspection procedures, which are eliminated in a voluntary manner immediately after the State inspector's warning. On the other hand, this is also due to the case law which confirms that before the Commissioner issues its decision, ordering the termination of such processing and the erasure of unlawfully collected personal data, the Commissioner must notify the person liable on the reasons why it believes there is no legal basis for the said processing and which arguments confirm such standing (the principle of examination of parties from Article 9 of the ZUP).

Thus, according to the case law, before the regulatory decision is issued, the person liable has the right to be heard regarding the Commissioner's standpoint. This means, in practice, that in the majority of cases the persons liable will, after hearing the Commissioner's arguments, erase personal data that had been collected unlawfully themselves or will stop with the unlawful processing of personal data. For this reason, issuing a regulatory decision is no longer necessary.

In the course of inspection proceedings, the Information Commissioner found that the established violations are predominantly due to the ignorance or misunderstanding of the legislation. To a lesser extent, they are due to the negligence or deliberate cheating and violations of legislation. The deliberate violations of legislation are noticeable particularly in the private sector due to the economic interests of offenders, which is evident especially with the unlawful use of personal data for direct marketing purposes.

Persons liable who perform their activities in fictitious business premises present a big problem in the process of inspection procedure. In such cases, there is usually only a mailbox at the company's headquarters (usually one single mailbox for several similar companies at the same time), and the company's activities are carried out via the Internet. As a rule, there are no employees in such companies, and usually responsible persons are not citizens of the Republic of Slovenia, many times they are not even citizens of the EU Member States. During the on-site visits of State inspectors, it was found that such companies usually do not accept postal items, as mailboxes are literally filled up with the delivery confirmation notices, so it is impossible to conduct the procedure against them. It is even more complicated in cases when responsible persons are not citizens of the Republic of Slovenia; they never accept postal items, so it is in fact impossible to serve them with the postal deliveries. Equally unsuccessful is the enforcement of unpaid fines when it comes to foreign nationals, where a question arises whether they are even real persons.

The Information Commissioner is convinced that such a situation enables unlawful conduct of companies and the avoidance of responsibility for committed offenses, which causes concrete economic damage to the Republic of Slovenia and its people. For this reason, the Commissioner turned to the Ministry of Justice and the Ministry of Economic Development and Technology with an initiative that the said ministries examine the above mentioned issues and consider the possible measures that would oblige the companies to conduct their business lawfully, which would require a change of legislation. According to the Information Commissioner, it would be possible to regulate this issue with the amendments to the Companies Act and/or the Minor Offences Act. In particular, the Information Commissioner believes it would be useful (at the very least) to introduce the institution of an authorized person for serving the documents of State bodies of the Republic of Slovenia in the territory of our country. The Commissioner is convinced that the current situation is a bad example to many similar companies that look for ways to circumvent the legal provisions in the future.

The Information Commissioner continued to participate in the drafting of the Minor Offences Act (ZP-1) in 2015 and proposed to the Ministry of Justice the amendment of the aforementioned Act in part that relates to the imposition of fines for concurrent offences. The Supreme Court of the Republic of Slovenia, in its judgment No. IV Ips 51/2011 of 21 June 2011, relating to the concurrence of offenses in the event of unlawful processing of personal data, stated that "in cases of such offenses, there are as many offenses as there are injured parties" and that "any interference with the individual's right to information privacy constitutes a stand-alone offense." The Information Commissioner welcomes such an interpretation, but at the same time draws attention to the difficulties of imposing such fines in practice. In the absence of the power of the Information Commissioner to impose a fine that would be lower than the minimum prescribed for (ideal or real) concurrence of offences, the Commissioner may only impose a fine that is a multiplication between the minimum prescribed fine and the number of individuals that were subject to violation of personal data protection. A single fine imposed on the medium and large legal entities can thus amount to a million Euros, while for the responsible persons of legal entities, sole proprietors and responsible persons of State bodies and self-governing local communities the fine amounts to 20,000 Euros. For example, the Information Commissioner has, in recent years, issued several minor offense decisions, by which it imposed a maximum total fine in the amount of EUR 20,000 to responsible persons of State bodies due to a large number of unlawful consultations into the data filing systems. The Commissioner imposed a fine of EUR 300,000 on the sole proprietor due to the unlawful processing of personal data of large numbers of individuals. The Information Commissioner believes that such (excessive) fines go beyond the needs for a punitive policy in this field. In such cases, the offenders usually file requests for judicial protection, as the current legislation only allows the courts the possibility to impose fines outside the prescribed minimum limit according to the ZVOP-1. However, the offenders encounter an additional obstacle before the courts, because the practice of

the courts is not uniform. In certain cases, the courts will reduce a high fine that was imposed, while in other cases they will not. However, it is currently impossible to determine what led the courts to such different decisions. Therefore, the Information Commissioner insists that an appropriate legal solution should be found, according to which the Commissioner would be permitted, as a minor offence body, to impose a fine lower than the minimum prescribed for a particular offense in the event of a concurrence of offences. In accordance with the provisions of Article 26 of the ZP-1, only the courts, not the minor offence body may currently impose a fine lower than the minimum prescribed.

The Information Commissioner considers that in the last 10 years of its operation, both the general and the professional public's awareness of privacy and data protection improved significantly. Data controllers are relatively well aware of their duties, but nevertheless violations still occur and this calls for both preventive and inspection activities. Privacy protection requires constant awareness raising activities.

In spite of the comparatively good awareness of personal data protection (at least according to European surveys), the Information Commissioner finds that due to the rapid development of technology, occasionally a misunderstanding of the right to privacy and data protection occurs. The wide expansion of social networks such as Facebook and Twitter and other online services for publishing and sharing of data and for instant messaging (Instagram, Snapchat, WhatsApp) and their constant availability through mobile devices, give many people the impression that privacy as a social norm is a thing of the past. We live in times when many people share vast amounts of information about themselves and their close ones with the public on the Internet, we read about mass and ubiquitous eavesdropping, and the drones hovering above us invade our spatial, communication and information privacy. Many people are reasonably worried that the battle for privacy is lost. Many often still believe that privacy is meant to hide something bad, and that one does not need the protection of privacy and personal data if he/she has done nothing wrong. Data protection is sometimes a simple target and an excuse to conceal the lack of knowledge about the legislation and the arguments that if we protect personal data, it will be impossible to protect other rights and interests. The Information Commissioner is aware that the protection of privacy in the information society is a very difficult task, so much attention is devoted to balancing the rights and to raising awareness that it is not about hiding something bad, but about the power of informational self-determination. Additional awareness-raising activities in the area of privacy impact assessments and privacy by design is therefore an important goal. By this we could help data controllers understand that personal data protection is not an end in itself, and that it is not about rigorous prohibition of data processing, but that if they take an appropriate approach to personal data protection, this can be their competitive advantage and leverage in raising the trust of their clients. Often, the goals can be achieved without a disproportionate negative impact on individual's rights by data minimisation, short retention periods and taking similar measures. In spite of the large amount of work that has already been done, the guardians of privacy are, in a way, only at the beginning of their work, as the era of mass data processing has only just begun. The digitalisation of homes, cities and transport infrastructure will bring new large amounts of personal data. The implementation of the big data and the Internet of Things concepts present exceptional challenges for the protection of personal data, which will require constant monitoring and new tools for the protection of human rights.

In 2015, negotiations on the upcoming EU personal data protection regime had been finalized. A consensus has been reached on the reform of the legislative framework, embodied in the General Data Protection Regulation. With the expected final vote in 2016 and the entry into force in 2018, it will bring many changes to the field of personal data protection. There will be more emphasis given on the persons responsible for the protection of personal data, the personal data and privacy impact assessments, privacy by design, certification, more severe penalties and the inclusion of foreign data controllers that provide their services to European citizens. It will require from the supervisory authorities a wider and more intensive cooperation, which requires from the Information Commissioner to closely monitor the developments in this area. More emphasis will also be placed on the proactive demonstration of responsible practices and accountability, whereas it is even more important to constantly make efforts to raise awareness and be proactive.

In addition to a large number of individual opinions, the Information Commissioner issued a record number of guidelines and reports in 2015 as well. These documents deal with specific themes in the field of personal data protection, which give rise to a larger number of questions and dilemmas. The purpose of the guidelines is to provide data controllers in one place with key answers on issues from a particular thematic area. The Information Commissioner makes efforts to constantly improve the applicability of its guidelines, so they are mostly geared with useful tools, such as quick guides, checklists, examples of good and bad practices, tips

and answers to most frequent questions.

In 2015, the Information Commissioner issued the following guidelines:

• Guidelines on the implementation of video surveillance (new)

In the Republic of Slovenia, there are at least 1800 video surveillance providers - legal entities that have registered the video surveillance filing system in the Commissioner's Register of filing systems. It should be borne in mind that registering a filing system is not required from the private sector controllers that employ less than 50 employees, which means that in reality there are even more providers of video surveillance systems. These completely revised guidelines provide a number of clarifications and case studies and have been updated in light of the experience gained in the inspection procedures. Some of the important points regarding the implementation of video surveillance are the following:

- Video surveillance, conducted as a live video transmission, should be regarded as a form of video surveillance and are subject to the same obligations as cameras with connected recorders.
- Non-functioning (false) cameras do not constitute a violation of the provisions of the ZVOP-1, but the Information Commissioner nevertheless explicitly advises against using notices of video surveillance because these constitute an unfair, misleading, disproportionate and inappropriate measures.
- The individual / employee has the right to request the recordings from the video surveillance system in which he appears (the right to access one's own data).
- The video surveillance records can also be used as proof of possible violations of the rules on recording the working time.
- Recording employees who are not aware where the cameras are installed is forbidden. Such a rule also applies to companies that offer a service of mysterious purchases and want to record employees in the process.

• Guidelines on recording phone calls

"Your call is recorded for ensuring a higher quality of service," is a line we so often hear. Many suppliers of services and goods often record calls from people who want to obtain certain information, make a complaint, purchase goods, or call for help when someone is in trouble. We need to realise that recording phone calls represents an interference with the right to personal data protection of the caller, and an interference with the right to confidentiality of communications. It may therefore only be carried out in compliance with the Constitution and the laws. All forms of surveillance or interception of communications are forbidden or allowed only under precisely defined conditions, which the controllers do not respect in practice. The Information Commissioner and the Agency for Communication Networks and Services of the Republic of Slovenia (AKOS) thus prepared the guidelines aimed at clarifying the legal bases for the permissibility of recording telephone calls and providing recommendations in specific cases. Upon the adoption of these guidelines, the two bodies issued a notice that after a period of six months after the guidelines have been issued, the inspection supervision will intensify. The controllers therefore had a transitional period in order to eliminate the unlawfulness in recording the telephone calls. Recording is permissible if there is a need to provide evidence of the conclusion / modification of a transaction (for example, that there has been an order / a purchase / a complaint given over the phone) or if there is a legal basis for this (for example, recording calls to courts). However, it is not permissible to record calls where only general information is given, to record all calls, or to mislead with the recording for "disciplining" the callers.

• Guidelines on using GPS tracking devices

The systems of management and control of vehicle fleets rely increasingly on the built-in GPS tracking devices that have many possible uses for tracking the trucks, machinery, taxis, service vehicles, municipal wardens, postal workers and newspaper publishers, to monitor children, the elderly and the sick, the mountaineers ... Some employers also use the GPS devices to track the employees, although there is no explicit statutory regulation thereof. The guidelines therefore explain how to confirm whether the GPS is really needed, when the introduction of GPS tracking is proportionate and legitimate, and which safeguards are essential (e.g. the existence of legal basis, informing the employees). The use of GPS devices that collect employee location data will be subject to inspections in 2016.

• Guidelines on security of personal data

Security of personal data or information security is a fundamental element of personal data protection. Without proper procedures and measures to ensure information security, personal data may be lost, destroyed, processed without authorisation or otherwise misused. The new Commissioner's guidance

give advice separately for larger and smaller controllers, since the measures must be tailored to the risks involved. There are already a considerable number of internationally established standards, good practices and policies, such as ISO/IEC 27001 and COBIT standards, so the guidelines refer to them. In addition, larger data controllers may use an information security questionnaire as a help in ex officio inspections - controllers can prepare themselves for inspection with the help of this questionnaire and eliminate any deficiencies in personal data security in advance. The guidelines also provide examples of violations from the practice of conducting inspections, such as inadequate traceability of access to personal data or the loss of personal data. The guidelines for small controllers contain a quick information security guide, a checklist with basic safety requirements, practical guidance, tips, and good practice examples.

- Guidelines on contractual processing of personal data

Hiring cloud computing services, accountancy services, call centres, application maintenance services and outsourcing of direct marketing are examples of contractual processing of personal data. In this area, the Information Commissioner receives a large number of requests for opinions and it takes stock of which problems arise in practice. The so-called successive (sub-)processing may be particularly problematic because a data controller may lose control of the personal data that it processes. In the guidelines, therefore, we clarify what the concept of contractual processing means, what are the obligations of data controllers and processors, what sort of pitfalls we may expect and we present recommendations on how to be compliant with the legislation when outsourcing the services which include processing of personal data.

As the data exchange agreement with the US - Safe Harbor - has been annulled, the Information Commissioner renewed three guidelines in 2015 that touch upon this area, namely:

- The Guidelines on personal data transfers,
- Protection of personal data and cloud computing, and
- Cloud computing - a summary for small businesses.

In addition to the guidelines, the Information Commissioner also publishes reports that aim at highlighting certain areas of data collection and processing that in the Commissioner's view deserve a special attention. The information society enables different and always new ways of data collection, so in the absence of a normative regulation, it is even more important that we understand such data processing. The Information Commissioner's reports highlight the characteristics and risks of such processing of personal data in the hopes of enabling a better understanding of the basic principles of personal data protection and privacy, and to initiate an appropriate response both in the professional and general public. Without a proper awareness and understanding of these concepts in the area of new technologies, our fundamental rights will become increasingly difficult to protect. One such example is certainly the use of unmanned aerial vehicles (drones). In the report on drones, the Commissioner discusses the risks to human rights, particularly to the right to privacy that the increasing use of this technology brings. The report describes the strengths and risks the drones pose for privacy, and makes recommendations to the legislator, the operators and individuals. The Information Commissioner wanted to encourage a public debate by publishing this report and urged the legislator to prepare the appropriate legislation, without which we may face uncontrolled and extensive infringements of human rights.

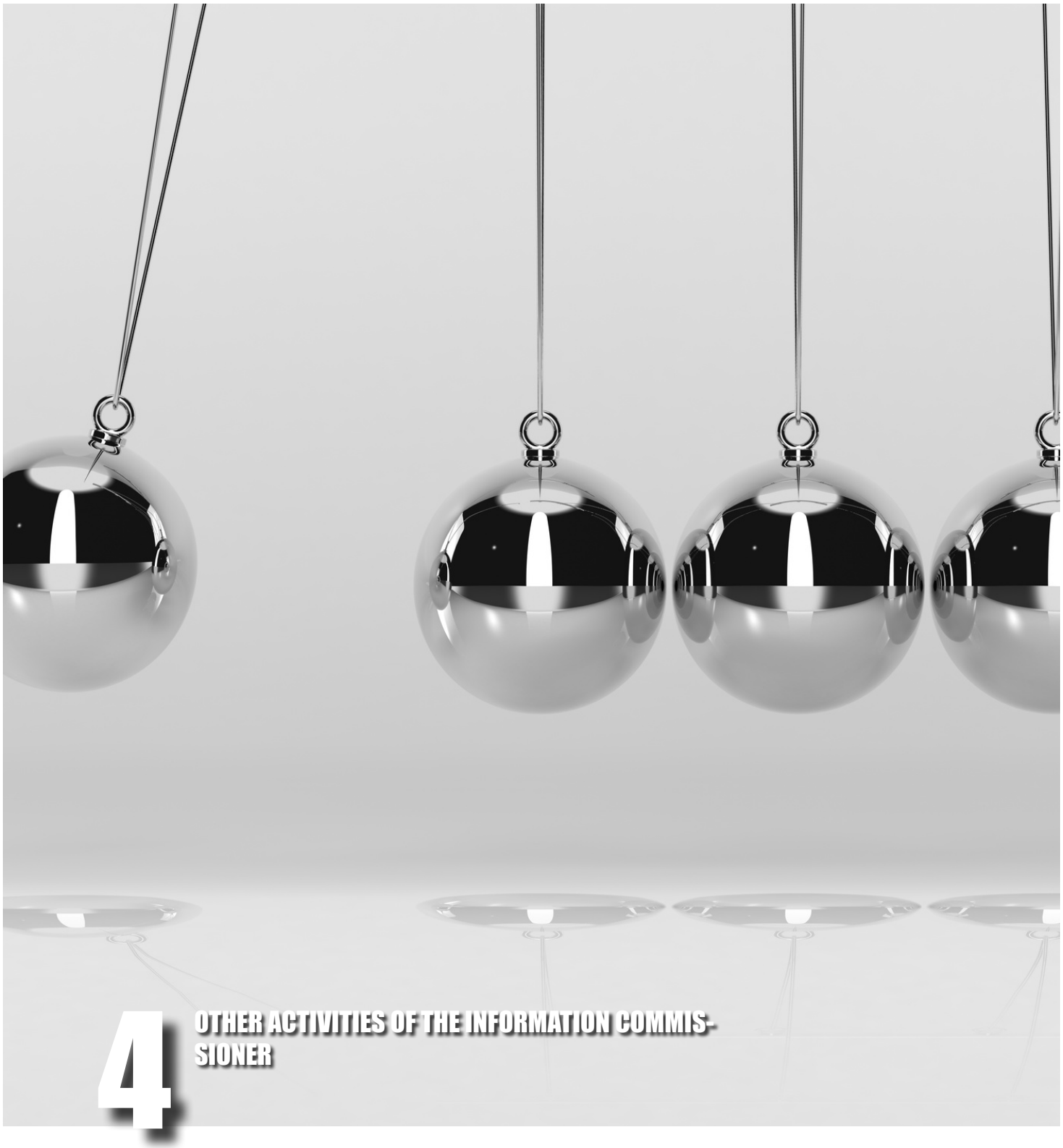
The Information Commissioner also assists informally in the performance of privacy impact assessments as one of the basic tools for a timely approach to an adequate protection of personal data. In 2015, more than 100 controllers and processors from the public and the private sector contacted the Information 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 privacy and personal data protection assessments, according to the Information Commissioner, have a major preventive effect. Namely, when such assessments are performed, there are fewer inspection measures needed, fewer violations found, and data controllers have lower costs due to imposed sanctions, loss of reputation and loss of consumer confidence.

In addition to the privacy impact assessments, the Information Commissioner also performs trainings for public sector controllers, including ministries, municipalities, administrative units, other State bodies and major data controllers. In 2015, the Commissioner carried out education courses for a wide ranging professional public (e.g. business representatives, representatives of educational, health, non-governmental organizations, autonomous and independent State bodies, judicial experts, societies, journalists, students from various faculties, etc.) and public sector controllers (e.g. the National Assembly, courts, faculties, the

Ministry of Public Administration, the Ministry of Education, Science and Sport, the Employment Service and the Institute for Pension and Disability Insurance). The primary purpose of such trainings is to enhance the level of personal data protection when drafting regulations or introducing appropriate system solutions.

The Information Commissioner's experts raise awareness on the importance of privacy and personal data protection at various conferences and professional events. In 2015, they took part in INFOSEK 2015 and SMARTDOC 2015 conferences, the Budapest Drone Conference, the EU28 Cloud Security Conference, Mobile Phone Safety, the Public Sector Efficiency Conference, the Consultation on the use of unmanned aerial vehicles, the Criminal Law Days, the Open Data Festival and others.

The Information Commissioner exercises its preventive functions through professional cooperation in 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, participation in the project of renewal of the national eGovernment portal and cooperation in the drafting of the regulation on information security policy for the public sector.



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 2015, the Information Commissioner issued more than 100 opinions on amendments to the laws and draft laws. The Commissioner noted also that there is no decrease of 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.

Some of the acts and regulations that the Commissioner gave its comments on in 2015 include:

- Public Employees Act,
- Police Tasks And Powers Act,
- Proposal of the Act Amending the Agricultural Land Act,
- Proposal of the Prevention of Money Laundering and Terrorist Financing Act,
- Proposal of the Act Amending the Public Information Access Act,
- The Act Amending the Tax Procedure Act,
- Proposal of the Act Amending the Companies Act,
- Proposal of the Act Amending the Electronic Communications Act,
- Draft of the Act Amending the Media Act,
- Proposal of the Act amending the Criminal Procedure Act (ZKP-N),
- Proposal of the Act Amending the Copyright and Related Rights Act,
- The Minor Offences Act,
- The Environmental Protection Act,
- The Act Amending the Housing Act,
- Proposal of the Act Amending the Gaming Act,
- Proposal of the Banking Act,
- The Act Regulating the Obtaining and Transplantation of Human Body Parts for the Purposes of Medical Treatment,
- The Cultural Heritage Protection Act,
- Proposal of the Residence Registration Act,
- The Chimney Sweeping Services Act.

4.2 Relations with the public

Throughout 2015, the Information Commissioner provided for the publicity of its work and 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 entities and persons liable; furthermore, it participated in a number of conferences, workshops, and round tables. The Commissioner also communicates via social media, through its Facebook profile. 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, the Commissioner conducted a number of lectures on the protection of personal data on the Internet for schoolchildren, teachers and parents. The Information Commissioner continued its preventive activities and dedicated a great deal of attention to disseminating tools and aids for raising awareness. In addition to the Annual Report for 2014, the Commissioner released the following guidelines: the Guidelines on the implementation of video surveillance, the Guidelines on contractual processing of personal data, the Guidelines on telephone call recording, the Guidelines on the protection of personal data in relation to the use of GPS devices, the Guidelines on personal data protection and the Report on the use of unmanned aerial vehicles from the point of view of the protection of fundamental human rights and the leaflet Practitioner for the protection of personal data.

The Information Commissioner also marked the European Personal Data Protection Day (28 January) and organised an event entitled Protection of personal data in practice and dedicated the event to the elderly. The event was organised in cooperation with the Slovenian Computer Emergency Response Team SI CERT and the social enterprise Simbioza Genesis. The Commissioner explained the participants how to safely use the Internet and e-mail, and informed them about the right to access their own personal data (for example, when and how they can consult their medical records) and about their other rights (e.g. how to avoid or prevent harassment over the phone). The Information Commissioner prepared a leaflet with useful instructions and advice on privacy protection and it awarded a good practice award in the field of personal data protection, which is now already an established tradition. The award was given out to the Ministry of the Interior with an explanation that the Information Commissioner, in the framework of the regular review under the Eurodac Regulation, checked the lawfulness of processing and personal data protection in the Eurodac database, without finding any irregularities. The Commissioner awarded the Ambassador of Privacy award to the high-tech company Alpineon, d.o.o., from Ljubljana, on the account that it implemented the concept of privacy by design into their SmartPARK system, which provides energy-efficient and environmentally friendly optimized management of smart parking systems. The Commissioner also awarded seven companies that acquired the ISO/IEC 27001 certificate on information security in 2014, by which they demonstrated a high level of protection of personal data.

On the occasion of the International Right to Know Day (on 28 September), the Information Commissioner organized the public consultation under the title Public information in the service of quality of life. The event was dedicated to the questions of access to public information in areas that significantly contribute to raising the quality of life of individuals (namely, public health, drinking water, environmental protection, consumer protection) and the involvement of individuals and civil society in the decision-making processes of public sector bodies in these areas. The Information Commissioner organized the event in cooperation with the Legal Informational Centre for NGOs - PIC. The participants of the event, led by the Information Commissioner Mojca Prelesnik, were the Ombudsman, a constitutional law professor, a senior judge at the Administrative Court, representatives of the Ministry of the Environment and Spatial Planning, the National Institute of Public Health, the Slovenian Consumers' Association and non-governmental organizations. The Information Commissioner awarded the Ambassador of Transparency award for good practice in the field of access to public information. The Municipality of Velenje received the award on account of large volumes of quality environmental information and documents published on its user-friendly website, as well as due to the efforts to ensure transparent access to data on activities of the municipality in the field of environmental protection.

4.3 International cooperation

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

In 2015, the Information Commissioner actively participated in seven EU working bodies engaged in supervision of the implementation of personal data protection within individual areas of the EU, namely the following:

- the Article 29 Working Party for personal data protection, as well as in four of its subgroups (the Future of Privacy Subgroup, the Technology Subgroup, the Binding Corporate Rules (BCR) Subgroup, and the Borders, Travel and Law Enforcement (BTLE) Subgroup);
- the Joint Supervisory Body for Europol;
- the Joint Supervisory Authority for Customs;
- the Joint Supervisory Authority for Schengen (SIS II);
- at the co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of CIS;
- at the co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of VIS;
- at the co-ordination meetings of the European Data Protection Supervisor (EDPS) together with state national authorities for the protection of personal data (EURODAC).

The Information Commissioner also actively participated in the International Working Group on Data Protection in Telecommunications (IWGDPT), which brings together the representatives of Information Commissioners and data protection and privacy authorities from all over the world. In 2015, 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).

The Information Commissioner answered 61 (the year before 49) questions and questionnaires from data protection authorities from abroad, international organizations, foreign academic and research institutions and non-governmental organizations. In February 2015, the Commissioner participated in an international inspection team, which supervised the protection of personal data at Eurojust at the Hague headquarters, and in May 2015 it participated in talks regarding the implementation of the imposed corrective measures.

In 2015, the Information Commissioner hosted representatives of similar institutions from Montenegro and Kosovo to whom it presented its activities and good practices in its fields of competence. In December, at the invitation of the Serbian Commissioner for Information of Public Importance and Personal Data Protection, the Information Commissioner attended an expert meeting in Belgrade with the purpose of exchanging experience in providing legal bases in sectoral legislation for personal data processing and of participating in the preparation of the European Data Protection Day.

The Information Commissioner's employees attended 16 international conferences, at some of which they delivered their contribution.

In 2015, 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. 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.