'14 Annual Report Information Commissioner

2014

'14 Annual Report

Information Commissioner

2014

0 INTRODUCTION

Dear reader,

Before you lies the Information Commissioner's Annual Report for 2014. In this year, the Information Commissioner issued a record number of decisions in the field of access to public information. Our work entails tackling ever new legal problems, but unfortunately we also deal with cases that should have never come to our attention as some of these problems should have been surpassed a long time ago.

In the field of access to public information, there is no doubt that the level of transparency among the public bodies has increased and that these bodies, due to public oversight, are more aware of their duties. Consequently, citizens are enabled a more efficient cooperation in decision making processes on things of public concern. Despite the progress, we notice that some public bodies still lack the awareness about their obligation to act transparently and that the citizens will only trust them if they will be properly informed about their work. The reflection on the lack of awareness is confirmed by numbers; last year, the Information Commissioner issued 280 appellate decisions in the field of access to information, the most in the last 10 years. The Commissioner received 578 appeals in 2014; 320 appeals were against refusals and 258 appeals against the non-responsiveness of the bodies. The Information Commissioner also received 297 requests for opinions and clarifications by both individuals and public bodies. In total, the Commissioner received and handled 875 issues. The number of appeals against the refusal decision of first instance bodies increased in 2014 in comparison to the previous year when the Commissioner received (only) 271 appeals.

A Consolidated Annual Report on the implementation of the Access to Public Information Act for 2014, adopted by the Government of the Republic of Slovenia, shows that the number of appeal procedures is in the decline. However, it is to be noted that the scope of the said Report is narrow and only covers the government sector, i.e. state and local self-government bodies, which is only around 500 entities, while on the other hand the Information Commissioner is competent for appeals against decisions of several thousand bodies. Since the number of appeals against the state and local self-government bodies declined, it is possible to conclude that the number of appeals against the bodies from the broader public sector increased.

In 2014, our work in this field was also marked by the adoption of the Amendment C of the Access to Public Information Act (APIA-C) that broadened the scope of bodies liable under this Act to include private entities subject to dominant influence of the public sector. The Information Commissioner notes that these "new" entities liable under the APIA lack awareness of their new obligations and, as a matter of rule, refuse access even to information that the Act considers absolutely public. As this is a completely new field with the praxis still developing, the Information Commissioner noted an increase in appeals in this field from April 2014 onwards.

The Commissioner estimates that the novelties brought about by the Amendment APIA-C demand that increased efforts are put into the promotion of the right to access public information and into trainings of the new entities liable under the Act on how to use the law in practice. In 2014, the Information Commissioner thus continued to implement different trainings and gave advice to liable bodies and requesters. Spreading the knowledge can effectively lower the number of those appeal procedures that emerge solely from the lack of communication between the requester and the body or from the lack of awareness of the law on access to information. As the appeal body, the Information Commissioner estimates that the level of awareness of the right to access public information on the part of requesters is good and thus they frequently exercise this constitutional right. At the same time, bodies liable under APIA still lack knowledge of their duties, among other reasons due to the lack of sufficient personnel and financing. For these reasons the Information Commissioner conducted trainings for the new entities liable under APIA-C and, in cooperation with the Ministry of Public Administration, issued a publication for these entities about their new obligations under APIA-C.

Despite the fact that in the recent years the public sector bodies strive for greater transparency, the Information Commissioner led procedures in several high-profile cases in 2014. Thus, the Commissioner ordered the release of contracts concluded by the Bank of Slovenia for performance of stress tests of the Slovenian banks. The Ministry of Finance had to release the information on the identity of the purchaser of state bonds issued in private placement. The City of Maribor was ordered the release the settlement agreement between the International University Sports Federation, Slovenian University Sports Federation and the City of Maribor relating to the damages agreed for the cancellation of the winter universiade. Furthermore, the Commissioner was called to determine the public nature of decisions of the Bank of Slovenia on emergency measures against five commercial banks recapitalised with public funds and established that these decisions ought to be public. The Commissioner also ordered the National Examinations Centre to release information on the overall success of each secondary school at the general baccalaureate. The Bank Asset Management Company was ordered to release the minutes of board meetings where the board members discussed the selection of external consultants and the Nova KBM bank, a business entity subject to dominant influence of public law entities, was ordered to release information on consulting, contractual or other intellectual services, which is information that is absolutely public according to the law. The Information Commissioner also granted the appeal of a journalist who demanded access to the transcript of the 69th regular session of the Government – the session in which the Government took note of the proposal for the nomination of candidates for the Commissioner of the European Commission. The Government denied the request based on the exemption of classified information and internal operations of the body, but the Information Commissioner reasoned that these exemptions are not applicable and thus the document ought to be released.

As of 2009, the Information Commissioner each year draws attention to the problem of charging of fees for the work of public officials related to access to information. The Commissioner believes that the fees for accessing documents should be kept at the lowest possible rate and should not cause a disproportionate obstacle for exercising the right to access public information. It is unacceptable that the fees for the work of public officials are charged based on hourly rate and are imposed on journalists and other requesters, even if the access to public information is not entirely free. This is due to the fact that the current system allows the bodies to charge only for material costs which undoubtedly do not cover the costs for the work of public officials who already receive salary from the budget.

The re-use of public information is a right that should hold a special place in the law on access to public information, although it is not fully operational in the Slovenian space. In 2014, the Information Commissioner considered eight appeal cases. Although this is more compared to the year before (when the Commissioner considered six appeals), the relatively low number of appeals shows, inter alia, that the requesters are not fully aware of the legal possibilities bestowed upon them in case the bodies liable refuse their request for re-use. The field of re-use of public information has an important economic potential which is, in practice, unfortunately still underexploited.

The Information Commissioner has an important role in preventing unlawful and unauthorised invasions in people's privacy and dignity while processing personal data. New technologies, in particular information technologies, have long since overcome the "traditional"

forms of collection, processing and publication of personal data and therefore significantly increased the threat to our privacy. A wide range of large and very indicative databases are created, whereas the data controllers are striving to make the best possible use of personal data for different purposes. Today, the right to privacy is now one of the most cherished human rights but, at the same time, it is also one of the most fragile rights due to the development of modern technologies and because the law always lags behind such a development. The requests received by the Commissioner increasingly relate to the issues connected with the use of these technologies: unauthorized video surveillance and audio recording, GPS tracking, monitoring the use of the internet and e-mails by employers, the use of biometrics, unlawful disclosure of e-mail addresses, direct marketing, cookies ...

In the field of personal data protection, the Information Commissioner led 628 inspection procedures, 95 minor offence procedures, four procedures on permissibility of implementation of biometric measures, 11 procedures regarding the issue of transfer of personal data to third countries, 14 procedures on linking different filing systems, 67 procedures on complaints with regard to the right to access individuals' personal data. As part of preventive activities in the field of personal data protection, the Information Commissioner cooperated with data controllers, consulted individuals and controllers orally and in writing, informed the public about all significant findings and developments in this area, and issued more than 2,000 written opinions.

This year was marked by some resounding cases of inspection, some of which are highlighted in this report. We recorded a significant increase of cases of unlawful video surveillance and audio recording and this trend is also reflected in high numbers of requests for opinions and complaints. The question of lawfulness of recording conversations and debates at sessions and meetings was frequently addressed as there is no explicit legal basis in the law for such recording and such recording is only permissible on the basis of the individuals' prior consent. This is because of the general rule that each interference with the right to personal data protection must have a legal basis. The basic premise of the right to protection of personal data is that each individual has the possibility to decide to whom and for what purposes he/she will allow access to their personal information. In the case of recording of interviews, meetings, sessions of municipal councils and other bodies, individuals must be given prior information on the data controller of such a recording, on the purposes for which the recordings will be used, how long will they be stored, who might have access to these recordings, etc. The development of technology and the fact that devices which enable voice recording are cheap and accessible to anyone, should not become a pretext for interference with the right to privacy and personal data protection, much less for the tolerance of such interferences. To the contrary, such developments require a careful consideration of the application of technology, which must not only comply with the law, but also with the human rights standards regarding privacy and personal data protection.

The incidents of invasion of privacy that echo in the public always reveal how severe such interferences are and how powerless can the individuals be. The expectations of the public are usually very high in such cases and it is difficult to explain the scope of Information Commissioner's competences. A sincere desire of all the employees at the Information Commissioner's Office is to help each individual, but this desire is sometimes not enough. Namely, the Commissioner must respect the principle of legality and can only act in accordance with the competences, bestowed upon it with law. One of such cases, where the public demanded the reaction of the Commissioner, was the publication of a video recording of a tragic incident at one of Maribor's (second largest Slovenian city) high schools. In this instance, there were elements to suspect that a criminal offence, not violation of the PDPA-1 has been committed. As the Commissioner had no competences to act in this case, we did not feel it would be appropriate to give our judgment in this case. Together with our colleagues we took the view that as a public sector body we should refrain from giving value judgments as the purpose of our work is not media recognition. We need to draw a line so that our work is done professionally and at an expert level, regardless whether a specific action is expected from us by the public and regardless of the concerns for visibility and likability.

Year 2014 also meant a turning point. This was mainly due to the judgment of the Court of Justice which for the first time recognised the search engines, specifically Google, as data controllers. This means that they too are subject the requirement to guarantee the deletion of inaccurate, outdated and incomplete data on individuals that search engines display in the search results. To ensure the rights of individuals, the search engine is required to "delist" the

names of individuals in search results, when specific conditions are met, in all the domains it operates in order for the individual's rights are effectively and fully protected.

The debates and concerns on the interferences to the right to privacy when using drones and sensory devices they may carry have become increasingly topical in 2014. The Commissioner takes the view that such debates and concerns clearly demonstrate the urgency of regulating this field both at the national and the European level. Only an adequate normative regulation can ensure the safe usage of these devices and at the same time the respect for fundamental human rights. We are convinced that the identification and control over drones in the airspace will not be possible without the system of administrative authorisations. The commercial use of drones demands new and efficient measures to protect personal data, such as prior impact assessments, new methods of informing individuals and strengthening the awareness rising activities aimed at drone operators which may be part of the system of issuing the relevant licenses.

One of the more pressing challenges for the protection of personal data protection comes in the form of "big data" where large quantities of complex and usually unstructured data from various sources are being processed. Such data and the analysis stemming from it is then used for the purposes of identification and prediction of trends and correlations. Big data offers great opportunities and can, for instance, be used to map epidemics, discover the correlations between the effects of different drugs, create detailed profiles of persons of interest, or be used as input for machine learning and decision-making algorithms. In the era of data abundance, it is even more important, even urgent, to draw attention to the basic principles of data protection, such as minimisation and proportionality of processing, the purpose limitation principle, transparency and the rights of individuals to access their personal data. Disregarding these basic principles could lead to an increased profiling and automatic decision-making practices, such as in relation to the question whether an individual is creditworthy or eligible to get a specific job; what kind of health insurance will we be able to secure; and what type of deals for energy and telecommunication services will we be offered.

The Information Commissioner takes very seriously the activities related to ensuring a systemic approach to guaranteeing the right of personal data protection and cooperating with relevant ministries in the process of drafting laws and regulations that touch upon the right of personal data protection. The goals of these activities are to ensure the legality of processing of personal data, especially when new forms and ways of processing emerge, and when it comes to establishing new data filing systems. Unfortunately, the Commissioner noted the continuation of a trend of preparing draft laws that present serious interferences with the right to privacy due to envisaged data processing without adequate analyses and assessment of the consequences to the constitutionally guaranteed protection of privacy. Several ministries adopted a practice of not sending the draft laws to the Information Commissioner for coordination and its opinion, which later causes troubles in practice and even the need for constitutional reviews of such laws. One of such laws was the Electronic Communications Act for which the Commissioner requested a constitutional review in relation to the mandatory retention of electronic communication data. In July 2014, the Constitutional Court declared the data retention regime set by the Electronic Communications Act unconstitutional. The Commissioner was greatly pleased by this decision as it represented a very important step towards the protection of individuals' privacy. The Constitutional Court recognised the importance of personal data protection in relation to modern communication technologies, in particular when these are used by state repressive bodies or the purpose of their use is to enable them to execute their powers. This decision also represents an important addition to the debates on the necessity and proportionality of the use of surveillance technologies in the context of criminal procedures and the intelligence services' activities. The Information Commissioner frequently draws attention to the problem of excessive interferences by state bodies into individuals' privacy. One of the most worrying practices in this regard is bulk collection of personal data of all people in order to identify one perpetrator of criminal acts or minor offences. Such a practice interferes with privacy rights of everyone, mostly those people who respect the rules and give no reason to state to act against them. As a rule, easier access to new technologies led to the troubles with introducing new powers of the law enforcement bodies. In practice, we are mainly speaking about drones and IMSI-catchers.

The Commissioner considers international cooperation as a very important element for ensuring the quality of its work. However, the year 2014 was marked by budget savings and thus the Commissioner's employees only participated and contributed in international semi-

nars and conferences in most urgent cases. The Information Commissioner has regularly participated in the Working Group 29, which brings together all European data protection guardians and provides the European Commission its expertise in the field of personal data protection. Due to budget cuts, we only attended plenary meetings of the Working Group 29 and meetings of four of its otherwise numerous subgroups. In addition, the Information Commissioner, as a supervisory body for specific areas of the processing of personal data, took part in only the most urgent plenary meetings of the supervisory bodies for Schengen Information System, Europol, Customs Information System and Eurodac. We also participated in the meetings of the International Working Group on Telecommunications (IWGDPT) and the TP-D committee at the Council of Europe.

For many years, the Information Commissioner has been systematically monitoring the practice and gathering feedback in relation to various issues. This leads to issuing the Commissioner's guidelines which in practice have proved as very useful tools, both for data controllers and individuals alike. Following this practice, the Commissioner issued several guidelines also in 2014; namely we touched upon the issue of (in)admissibility of using GPS tracking devices, while special focus was given to the necessity of conducting a prior privacy impact assessment when introducing new police powers. Despite the fact that many issues have already been addressed, the Commissioner is facing many challenges emerging from the present day conditions. We also have to deal with the lack of legal norms regulating the processing of personal data with new technologies. These are no longer science fiction: drones, smart video surveillance, the internet of things, Trojan horses, big data, automatic license plate recognition, new forms of biometrics, increasingly smart phones and devices, infinite possibilities of profiling and automated decision-making. The existing legal basis no longer fits the contemporary way of life, shaped by modern technologies; these give us a lot, but in return they demand vast amounts of our personal data. For this reason, the new General Data Protection Regulation is being negotiated at the EU level. It brings many new concepts and obligations for the controllers, will it aims to give more rights to individuals, including the so-called right to be forgotten or, better said, the right to demand deletion of personal data processed without a legal basis. The principle of data by design will finally find its place. This principle reminds us that personal data protection should be kept in mind before any processing, i.e. before the introduction of new measures and data-processing systems, and not only after the individual has already suffered damage.

In lieu of conclusion: the right to access of public information and the right to personal data protection are two fundamental human rights, guaranteed by the Constitution. Let's be proud of them and let's demand that they are realised to the greatest possible extent. Both have an important role in a society and are a great indicator of its democratic nature. Most notably, they are a result of centuries of societal development and priceless values.

Mojca Prelesnik,
The Information Commissioner

INTRODUCTION

1 THE INFORMATION COMMISSIONER

1.1. The Establishment of the Information Commissioner

On 30 November 2005 the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act (hereinafter the ICA),[1] by means of which a new and independent state authority was established as of 31 December 2005. The Act combined two authorities, namely the Commissioner for Access to Public Information, which was an independent institution even before the merger, and the Inspectorate for Personal Data Protection. Since the ICA entered into force, the Commissioner for Access to Public Information continued its work as the Information Commissioner, taking over the inspectors and other employees of the Inspectorate for Personal Data Protection, the equipment and assets. At the same time, it took over all the uncompleted tasks, archive and records of the Inspectorate for Personal Data Protection. Therefore, the activities of the body responsible for the protection of the right to access to public information changed significantly and spread into the field of personal data protection. The Information Commissioner thus became the national supervisory authority for data protection. This newly established authority commenced its work on 1 January 2006.

Such a system, comparable to the system of some developed European countries, helped unify the practice of both bodies and spread the awareness of both the right to privacy and the right to know; these two rights coexist even more effectively thanks to this system of protection.

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 a functionary 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; funding is allocated by the National Assembly of the Republic of Slovenia on the proposal of the Information Commissioner.

The position of the Information Commissioner was held by Nataša Pirc Musar since the establishment of the body until 17. 7. 2014. On this day, the former Commissioner handed over the business to the new Information Commissioner, Mojca Prelesnik, who thus started her five-year mandate.

1.2 The Competences of the Information Commissioner

The Information Commissioner performs its statutory tasks and competencies in two fields:
1. The field of access to public information;
2. The field of personal data protection.

In the **area of access to public information**, the Information Commissioner acts as the appeal body, competent for deciding on the appeals against the decisions by which another body has refused or dismissed the applicant's request for access, or violated the right to access or re-use public information; in the context of appellate proceeding the Information Commissioner is also responsible for supervising the implementation of the Act governing access to public information and regulations adopted within the framework of appellate proceedings.

In the area of access to public information, the Information Commissioner also has the competences determined by the Media Act (Article 45).[2] A liable authority's refusal

1 Official Gazette RS, Nos. 113/05 and 51/07 – ZUstS-A.
2 Official Gazette RS, No. 110/2006 – official consolidated text 1, with amendments.

of a request by a representative of the media shall be deemed a decision refusing the request. The failure to respond to the request is considered both a misdemeanour and the reason for the appeal. The authority competent to decide on appeals is the Information Commissioner who considers the appeal in accordance with the provision of the Access to Public Information Act (hereinafter the APIA).[3]

In the area of personal data protection, the Information Commissioner acts according to the competencies as defined by the Personal Data Protection Act and Article 2 of the ICA. namely:

1. performing supervision over the implementation of the provisions of Personal data protection Act (PDPA) and other laws that regulate the processing of personal data (handle cases of complaints, appeals, notifications and other applications, explaining possible breach of law and perform planned-preventive inspections with personal data controllers in public and private sectors);
2. deciding as appellate body on individuals' complaints when controller of personal data refuses his/her request for access to data relating to him/her or request for extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the act governing personal data protection;
3. performing procedures with regard to violations in the field of personal data protection (expedient procedure);
4. managing and maintaining a register of filing systems, ensuring its updating and public internet access (Art. 28 of PDPA);
5. ensuring viewing and transcription of data from the register of filing systems (as a rule on the same day or in eight days at the latest – Art. 29 of PDPA);
6. deciding on an individual's complaint with regard to processing of personal data based on Art. 9(4) and Art. 10(3) of PDPA;
7. issuing decisions on ensuring an adequate level of personal data protection in third countries (Art. 63 of PDPA);
8. performing procedures for assessing an adequate level of personal data protection in third countries based on findings of supervisions and other information (Art. 64 of PDPA);
9. managing a list of third countries ascertained to have partially or entirely adequate or inadequate personal data protection levels; in case only a partial adequacy of personal data protection is ascertained, the list will also state the scope of adequate protection (Art. 66 of PDPA).
10. managing administrative procedures to issue permissions to transfer personal data to a third country (Art. 70 of PDPA);
11. managing administrative procedures to issue permissions to link public records and registers when one of the filing systems to be linked contains sensitive personal data or if implementation of the linking requires the use of the same connecting code (such as the standardized personal registration number or tax number) (Art. 84 of PDPA);
12. managing administrative procedures to issue declaring decisions on whether a planned implementation of biometric measures in private sector is accordant with the provisions of PDPA (Art. 80 of PDPA);
13. cooperating with government bodies, competent EU bodies for protection of individuals with regard to processing personal data, international organizations, foreign personal data protection bodies, institutions, associations, and other bodies and organizations with regard to questions of personal data protection;
14. issuing and publishing preliminary opinions to state bodies and public powers holders on harmonizing the provisions of proposals of legislation with Acts and other legislation governing personal data;
15. issuing and publishing non-obligatory opinions on conformity of professional ethics codes, general conditions of business or the proposals thereof, with regulations in the field of personal data protection;
16. preparing, issuing and publishing non-obligatory recommendations and instructions with regard to personal data protection in a particular field;

3 Official Gazette RS, No. 51/2006 – official consolidated text 2, with amendments.

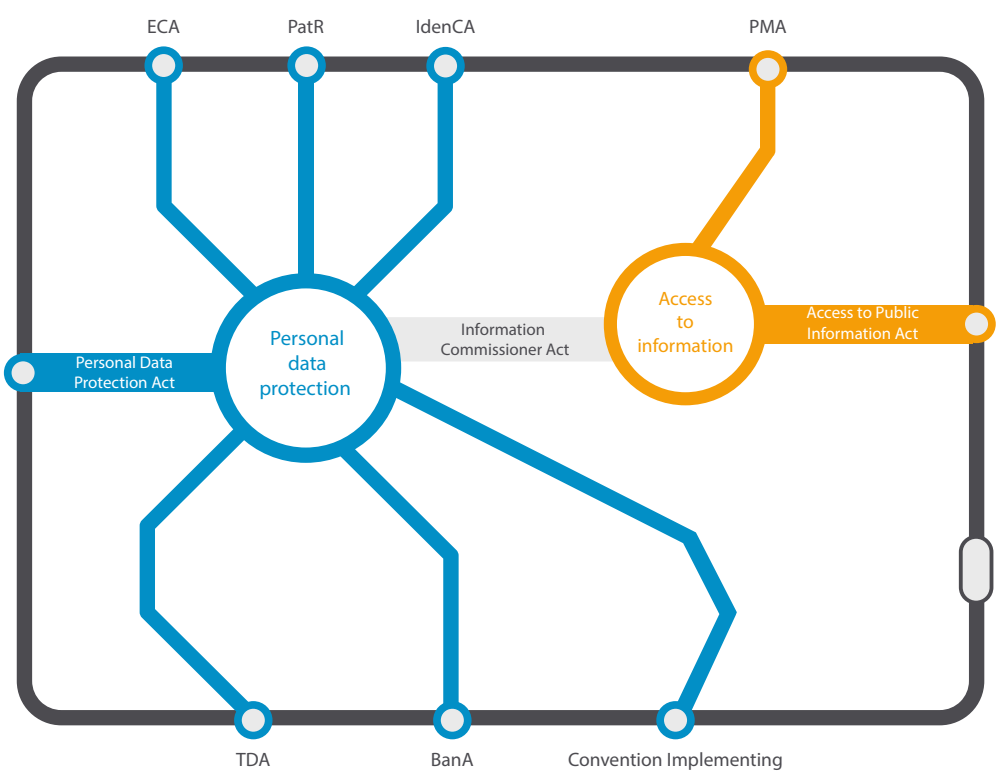
17. the publication on the internet page or in another appropriate manner of preliminary opinions on compliance with positive Acts and other legislation of proposals of Acts and other regulations in the field of personal data protection as well as publication of requests for constitutional review of statutes (Art. 48 of PDPA), issue internal bulletin and expert publications, publish decisions and court resolutions dealing with personal data protection, as well as non-obligatory opinions, explanations, positions and recommendations with regard to personal data protection (Art. 49 of PDPA);
18. issuing press releases on performed supervisions and prepare annual reports on its work in the current year;
19. participates in working groups for personal data protection, formed within the EU framework and bringing together independent bodies for protection of personal data in member states (Working party 29 based on Directive 95/46/EC; supervisory bodies dealing with processing of personal data in Schengen information system, Customs information system and Europol; and Eurodac Supervision Coordination Group).

The Information Commissioner is an appellate body, competent for supervision over implementation of the Information Commissioner Act, the Access to Public Information Act within the frame of its appellate proceedings, the Media Act and the Personal Data Protection Act.

The Information Commissioner is entitled to request from the Constitutional Court to initiate the procedure for the review of the constitutionality or legality of regulations or general acts issued for the exercise of public authority, provided that a question of constitutionality or legality arises in connection with a procedure the Commissioner is conducting.

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

Figure 1: Competences of the Information Commissioner.



The Information Commissioner is competent under the Patients Rights Act[4] (in relation to accessing medical records), the Travel Documents of Citizens of the Republic of Slovenia Act[5], the Identity Card Act[6] (in relation to photocopying personal identity documents), the Banking Act[7] (in relation to the supervision of personal data processing within the SISBON system) and the Consumer Credit Act.[8]

The Information Commissioner also has competences under the Electronic Communications Act[9] which concern oversight over the provision 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 on disclosure of identification of the calling subscriber, the provisions on the use of cookies or similar technologies, and 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.

1.3 Organisational Structure and Budget of the Information Commissioner

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

- The Secretariat of the Information Commissioner;
- The Public Information Department;
- The Personal Data Protection Department;
- Administrative and Technical Services.

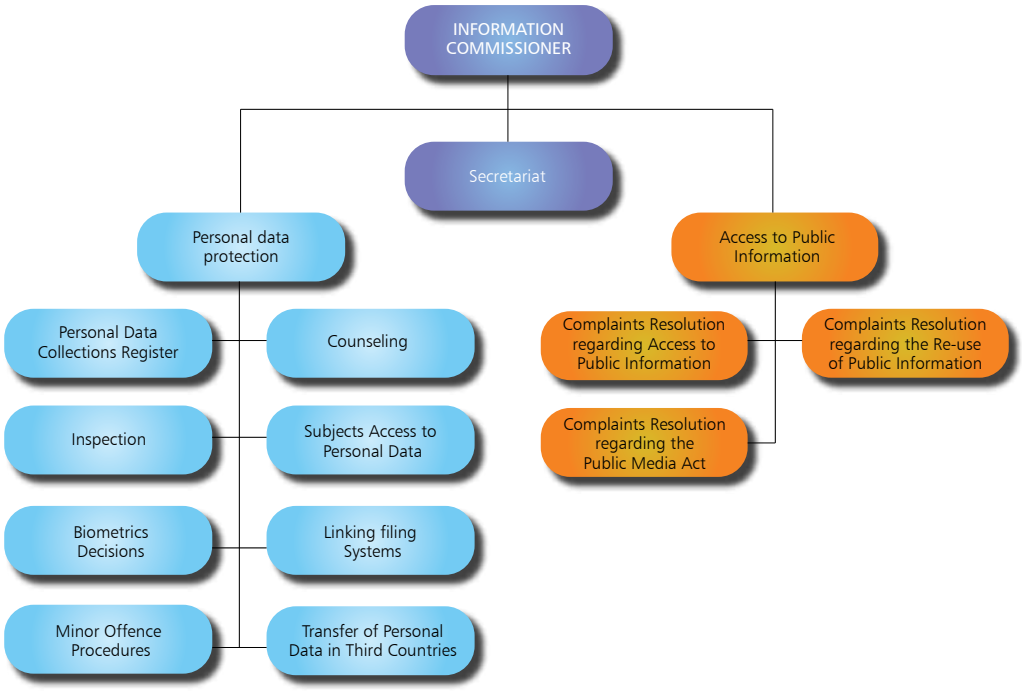
At the end of 2014, the Information Commissioner had 34 employees, of which three were employed on the basis of temporary contracts. The number of employees has increased by one person comparing to the previous year due to the anticipated increased workload emerging from the amended Access to Public Information Act (APIA-C).

The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia on the proposal of the Information Commissioner (Article 5 of the ICA). In fiscal year 2014, the funding allocated to the Information Commissioner at the start of the year amounted to EUR 1.247.110,10.

In 2014 EUR 1.069.962,25 were spent on wages and salaries. EUR 120.072,70 was spent on material costs and expenses. Material costs and expenses were necessary for the normal functioning of the Information Commissioner (stationery, travel expenses, cleaning expenses, student work payments, postal services, the education of employees, producing brochures, etc.).

4 Official Gazette RS, No. 15/2008; hereinafter: the PatRA.
5 Official Gazette RS, No. 62/2009 – official consolidated text 3; hereinafter: the TDA.
6 Official Gazette RS, No. 71/2008 – official consolidated text 2; hereinafter: the IdenCA.
7 Official Gazette RS, No. 131/2006 with amendments; hereinafter: the BanA.
8 Official Gazette RS, No. 59/10 with amendments.
9 Official Gazette RS, No. 13/2007 – official consolidated text 1, with amendments.

Figure 2: Organisational Chart of the Information Commissioner.



2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

2.1 Activities in the field of Access to Public Information

The right to access public information was ensured by legislators in the Constitution of the Republic of Slovenia. The second paragraph of Article 39 of the Constitution determines that everyone has the right to obtain information of a public nature in which they have a well-founded legal interest under law, except in circumstances as provided by the law. This right is further regulated in the Access to Public Information Act (hereinafter: APIA), which ensures everyone free access to and re-use of public information held by state authorities, local government authorities, public agencies, public funds, and other public law entities, bodies exercising public powers, and public service contractors. The Act came into force in March 2003.

The APIA has been significantly amended in 2014 with the Amendments APIA-C and APIA-D. The right of access to public information has been duly extended to include companies and other legal entities of private law and subject to direct or indirect dominant influence of the State, self-governing local communities and other entities of public law (the „new" bodies). The Agency for Public Legal Records and Related Services was tasked with establishing an online, free-of-charge public Registry of new bodies liable under the APIA. The aim of the amendments was to increase transparency and responsible management of public resources and financial resources of business entities subject to dominant influence of entities of public law. The Amendment C also expanded the scope of the obligation to provide information proactively on the websites of these private entities subject to dominant influence of the public sector.

The bodies liable under the APIA are therefore:

- State authorities, local government authorities, public agencies, public funds, and other public law entities, bodies exercising public powers, and public service contractors;
- Business entities subject to dominant influence of entities of public law.

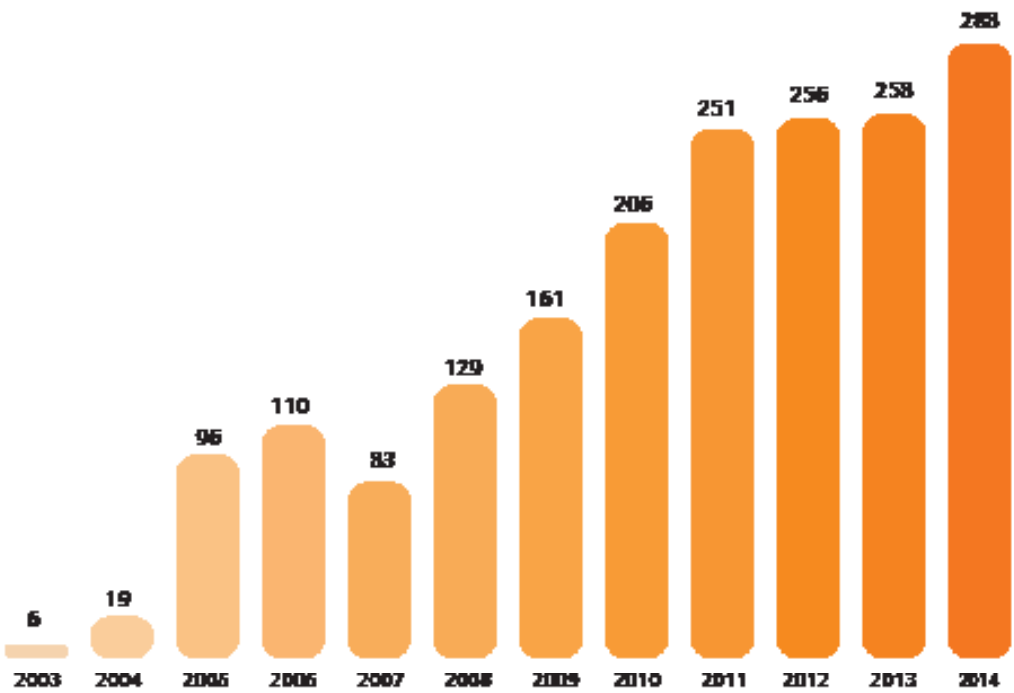
The definition of „public information" differs for the two groups of bodies liable under the APIA; it is narrower for the „new" bodies. While the notion of „public sector information" for the „traditional" bodies comprises all information in their possession, the reverse is true for business entities subject to dominant influence: information is considered „public information" only if the APIA specifies this explicitly. Such are, for instance, information on concluded legal transactions and information on representatives or membership in an administrative, management or supervisory body. There is another area where transparency obligations of business entities subject to dominant influence diverge from obligations of „traditional" public sector bodies: the obligation to provide public information is only applicable to information created while the entity was subject to dominant influence. In addition, entities subject to dominant influence may use a simplified procedure for deciding upon requests for public information; they are not obliged to issue a formal refusal decision so they are only required to inform the requester in writing of the reasons for not providing the requested information. Bodies that fall within both categories („traditional" and „new" bodies liable under APIA) are under the more stringent obligations applicable to the „traditional" bodies; they must issue a formal administrative decision.

In 2014, the Information Commissioner received 578 appeals, of which 320 were against decisions refusing requests, while 258 were against the non-responsiveness of first-instance authorities (the so-called administrative silence). In appeal proceedings against decisions in which responsible authorities rejected requests for access to or re-use of public information, the Information Commissioner issued 288 decisions (of which 53 cases had been submitted to the Information Commissioner prior to 2014). 25 cases concerned the right of access to documents held by business entities subject to dominant influence of entities of public law. Seven applicants withdrew their appeals, two appeals were dismissed by the Information Commissioner, and in one case matters were combined. In processing these appeals, 53 so-called in camera examinations were carried out by which the Information

Commissioner establishes the facts of the case in relation to the documents held by the responsible authority.

The following decisions were issued by the Information Commissioner:
- In 128 cases it dismissed the appeal as unfounded;
- In 84 cases it granted partial access to information;
- In 52 cases it granted the appeal in favour of the applicant;
- In 22 cases it returned the matter to the first-instance authority for reconsideration;
- In 2 cases the first instance decision was declared null and void.

Figure 3: The number of decisions issued in relation to access to public information from 2003 to 2014.



In its decisions the Information Commissioner made substantive rulings with consideration of the following:
- Whether the responsible authority actually possessed the document or the public information requested by the applicant (106 cases);
- Whether the documents requested contained personal data whose disclosure would result in a violation of personal data protection in accordance with zvop-1 (91 cases);
- Whether the applicant requested information or data deemed to be a trade secret in accordance with the legislation regulating commercial companies (54 cases);
- Whether a violation of procedural rules occurred (37 cases);
- Whether the information requested pertains to data in documents compiled in relation to the internal operations or activities of the authority and whose disclosure would interfere with the functioning or activities of the authority (34 cases);
- Whether the public interest in disclosure outweighs the public interest or the interest of other persons in restricting access to the information requested (24 cases);
- Whether the information requested pertains to data that was obtained or compiled on the basis of civil or non-contentious civil proceedings, or other judicial proceedings, and the disclosure of such would be harmful to the course of such proceedings (17 cases);
- Whether the body violated a substantive law (15);
- Whether the body is subject to dominant influence of the entities of public law (15);

- Whether the information requested pertains to data in documents that are in preparation and are thus still subject to internal consultation, and the disclosure of such documents would lead to misinterpretation of their content (14 cases);
- The issue of a decision in procedures in which the applicant requested documents related to public procurement procedures (14 cases);
- Whether the document requested meets the conditions for it to be deemed public information as provided for in the first paragraph of article 4 of APIA (13 cases);
- Whether the information requested relates to the work and personal information of public servants and officials (11 cases);
- Whether the authority correctly charged the fees for providing public information (11 cases);
- When the authority did not issue a decision to the applicant in relation to the requested documents, but provided them with public information that they did not even request (11 cases);
- Whether the information originates from the field of work of the authority (10 cases);
- 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 course of such proceedings (10 cases);
- Whether the authority to whom the request for access to public information was addressed to is in fact liable under the first paragraph of article 1 of APIA (9 cases);
- Whether the requested information pertains to data that was obtained or compiled for an administrative proceeding, whose disclosure would be harmful to the course of such proceedings (9 cases);
- Whether the case concerns the re-use of public information (8 cases);
- Whether the information requested pertains to data classified in accordance with legislation regulating classified information (8 cases);
- Whether the requested information is protected by copyright legislation - in such instances the applicant may be acquainted with the information by way of consultation on the spot (6 cases);
- Whether the applicant abused his/her rights under the APIA (6 case);
- Whether the requested information pertains to data whose disclosure would result in a violation of the confidentiality of a tax procedure or tax secrecy, in accordance with legislation regulating tax procedures (4 cases);
- Whether the case concerns environmental information (4 cases);
- The proactive publication of information (4 cases);
- Whether European Union law is involved (1 case);
- Whether the information relates to the issue of confidentiality of a source (1 case).

The Information Commissioner's decisions in appeal proceedings against refusal decision State authorities (115 cases), from which ministries, constituent bodies and administrative units (73 cases) and courts, State Prosecutor's Office and State Attorney's Office (29 cases),

- Public funds, public institutes, agencies, public service contractors, bodies exercising public powers and other public law entities (106 cases),
- Local government authorities (51 cases)
- Business entities subject to dominant influence of entities of public law (12 cases)

Four appeals concerned legal entity in the private sector; however, the Commissioner established that they are not liable under the APIA.

187 appeals were submitted by natural persons, 68 by private sector legal entities, 31 by journalists and 2 by public sector legal entities.

In 2014, the Information Commissioner received 258 appeals against the non-responsiveness of first-instance authorities. In these appeal proceedings, initiated due to non-responsiveness, the Information Commissioner first called on the responsible authority to decide on an applicant's request as soon as possible, which in most cases they did. In 30 cases the Information Commissioner rejected the appeal due to premature or incomplete applications, five applicants withdrew their appeals because they received the requested information, in 7 cases the Commissioner advised applicants that it was not competent to consider

their applications and transferred their cases to a competent authority for consideration.

An appeal against the decision of the Information Commissioner is not allowed, but it is possible to initiate an administrative dispute before the Administrative Court. In 2014, 29 administrative disputes were issued against decisions of the Information Commissioner (i.e. against 10.1% of all decisions issued). After a declining trend of disputes against the Commissioner's decisions was observed in the previous years, the share of disputed decisions grew slightly this year. In 2011, disputes were initiated against 13.1%, in 2012 against 10.5% and in 2013 against 8.1% of the decisions issued by the Information Commissioner. The reason for the increase in 2014 may be found in the lack of awareness of the „new" bodies liable under the APIA of their obligations or their practice of disputing the new obligations. 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 and the acceptance of the Information Commissioner's decisions by the authorities and the requesters.

In 2014, the Administrative Court issued 17 judgements in relation to appeals filed against decisions of the Information Commissioner in which it decided to:

- Dismiss the appeal as unfounded (8 cases),
- Grant the appeal, reverse or annul the decision in part or in its entirety and return the matter to the information commissioner for reconsideration (5 cases),
- Grant the appeal and partially set aside the commissioner's and the authority's decisions and refer the case back to the authority for reconsideration (2 cases),
- Grant the appeal, set aside the authority's decisions and refer the case back to the commissioner for reconsideration (1 case),
- Dismiss the appeal on procedural grounds (1 case).

The Administrative Court was asked to decide upon a request to rectify the operative part of the judgment („the sentence") issued in 2013, however, the Court dismissed the request.

In 2014, two requests for revision of the Administrative Court decisions were filed with the Supreme Court, although, by the end of 2014, the Supreme Court has not yet decided upon these requests. The Supreme Court did, however, decide on the request for revision filed in 2013 and dismissed it on procedural grounds.

In 2014, the Information Commissioner received 297 requests for assistance and various questions from individuals regarding access to public information, especially with regard to the question as to whether a certain document or information is considered public information. The Information Commissioner replied to all applicants within the framework of its competences, in most instances it referred applicants to the competent institution.

In 2014, two minor offence proceedings were initiated due to a violation of the first paragraph of Article 15 of ICA, wherein an authority failed to forward documents required by the Information Commissioner for the adoption of a decision in appeal proceedings. In both cases the Commissioner issued a monetary fine, whereas one person who committed the violation requested judicial review. The Information Commissioner also issued a warning in one case for violation of the Media Act. The Commissioner also reported several alleged violations of the General Administrative Procedure Act in conjunction with the APIA to the Inspectorate for Public Sector.

2.2 Most Significant Decisions of the Information Commissioner in Different Areas

Stress tests, business secret (No. 090-225/2013/4 of 13 January 2014)

The applicant requested a contract concluded by the Bank of Slovenia for the performance of stress tests and "AQR" with Ernst & Young, Deloitte, Oliver Wyman and Roland Berger. In the appeal procedure, the Commissioner found that the subject of the contract, financial terms, schedule of payments and the price are publicly available information under the law itself. Namely, the third paragraph of Article 6 of the APIA states that the information related to the use of public funds is absolutely public information. Furthermore, the Companies Act prevents companies from claiming their business secret in cases when a law provides that specific information shall be public. In addition, the Commissioner concluded that other parts of the requested information (parts that do not fall under the absolute public category of information) do not pass the "objective criteria" laid down in the Companies Act, whereby the information may be deemed business secret if releasing such information would cause considerable damage to the company. The threshold of harm for the exception of "internal functioning of the authority" to be applicable has also not been met in regard to all of the requested documents. However, certain parts of the contracts did meet the threshold to be considered a business secret and releasing certain other parts of the contracts would indeed cause harm to the internal functioning of the body. Finally, the contracts contain certain protected personal data that need to be redacted before providing the information to the requester. Thus, the Commissioner only partially granted the appeal and partially rejected it, ordering the body to grant the requester partial access.

Re-use of PSI (No. 090-263/2013/5 of 27 January 2014)

The applicant, a journalist, requested from the Agency for Public Legal Records and Related Services the entire Slovenian Business Register for the purposes of re-use for non-commercial purposes. The APIA stipulates that when requesting information for re-use, the applicant is required to state the purposes for which the information will be re-used (commercial or non-commercial purposes). The applicant stated that he requests the information on behalf of an international NGO for the purposes of conducting a research. The authority claimed that the applicant should have described in more detail the non-commercial purposes for which information is requested, namely what kind of a research is the applicant attempting to conduct. For this reason, the authority demanded that the applicant supplements his request and after he failed to do so, the authority dismissed his request as incomplete. The Commissioner, on the other hand, found that the request contained all the required elements and had thus been complete. The Commissioner decided that the authority must provide the requested information (the Slovenian Business Register) to the applicant for non-commercial purposes.

Personal data (No. 090-255/2013/9 of 14 February 2014)

The authority refused access to a legal opinion on compliance of the requirement of work experience in the process of selection of a candidate in an open tender. The opinion was commissioned by the Motorway Company of the Republic of Slovenia, the authority in this case. The Commissioner decided on appeal that the exception aimed at the protection of "civil, non-litigious civil procedure or other court proceedings" is not applicable in this case. Namely, the authority failed to prove the harm caused for a court proceeding should the information be released, neither did the Commissioner found any evidence to support the claim of harm. The Commissioner stressed that a court in its proceedings shall establish the veracity of claims made by the parties and decide on the basis of documents submitted by the parties, irrespective of whether the information in the court files is freely available to

the public or not. As regards the exemption of personal data protection, the Commissioner noted that in the document itself (the legal opinion), there are no personal information pertaining to individuals. Rather, the legal opinion includes general findings on how to interpret the notion of "work experience" in leading business positions and how such experience can be proven. The Commissioner found that the authority's decision was erroneous and that the applicant has the right to access the requested document. However, since the legal opinion is protected under the copyright legislation, the requester is only entitled to consult the document on the spot and may not receive photocopies.

Business secret (No. 090-1/2014/12 of 25 March 2014)

The applicant requested information from the Ministry of Finance on the identity of the purchaser of bonds issued in the private placement on 15 November 2013. The authority rejected the request relying on the business secret exemption and claiming that the release of this information would cause harm to the authority's internal functioning. The Commissioner found that the buyer himself does not consider his identity as a buyer a business secret, so the business secret exception cannot be relied upon. Furthermore, the exemption of "internal functioning" of the body is not applicable as no significant harm was established. Lastly, the Commissioner also noted that there are strong elements of public interest for the release of the requested information. The public interest lies in the need for transparent and open functioning of bodies and the need for responsible and diligent decision-making in relation to state borrowing as such decisions will affect the generations to come.

Proactive disclosure (No. 090-46/2014/8 of 12 April 2014)

The applicant requested photocopies of decisions of the Bank of Slovenia on emergency measures against all five commercial banks and the decision to terminate certain bonds which the applicant specified with exact annotations. The authority relied upon the following exemptions: business secret, personal data protection, protection of an administrative procedure and protection of internal functioning of the authority. It did, however, grant partial discloser of the requested documents. On appeal, the Commissioner noted that the authority later published all the decisions on emergency measures on its website in full. Thus, the Commissioner concluded that relying on the exceptions above is unfounded and it referred the applicant to the authority's website where the decisions had been published.

Document in the process of being drawn up and subject to consultation (No. 090-116/2014/3 of 12 June 2014)

The applicant requested from the Ministry of Justice access to expert opinions drawn by other public sector institutions in relation to the ratification of the Council of Europe Convention on preventing combating violence against women and domestic violence. The authority refused access in full, claiming that the documents are in the process of being drawn up and are still subject to consultation, whereas the disclosure of the documents would lead to misunderstanding of their contents. However, the Information Commissioner disagreed with this line of argumentation, noting that the requested information cannot be considered "unfinished", i.e. in the process of being drawn up. All the expert opinions had been concluded, signed and sent to the body. The fact that the body itself has not yet taken a final view on the matter of ratification does not mean that the expert opinions are unfinished. In addition, the Commissioner also conducted the specific harm test included in this particular exception and established that releasing the requested expert opinions could not lead to misunderstanding of their contents. What is more, the Commissioner drew attention to the proactive disclosure provisions of the APIA, whereby the bodies are required to publish, inter alia, opinions important in a general context or important in the course of the authority's decision making process, studies and other documents relating to the authority's field of work.

Internal operations of a public authority (No. 090-61/2014/6 of 13 June 2014)

The applicant requested information from the National Examinations Centre on the overall success of each secondary school at the general baccalaureate of 2011-2013 and the grades and scores received by the students of each of the secondary school (in an anonymised form). The Commissioner first established that the authority indeed possesses with this information as it is possible to recall such information (specified by categories) from the computerised database and the authority has the necessary equipment and expertise to retrieve the requested information. Moreover, the Commissioner found that the work put into retrieving this information would not mean creating new information, as the amount of work remains reasonable and not excessive. Thus, the Commissioner ordered the authority to provide the applicant with the requested information, as no exceptions have been found to be applicable.

Business entity subject to dominant influence, Business secret (No. 0902-6/2014/4 of 9 July 2014)

The applicant, a journalist, requested access to certain information from the Insurance Company Triglav, which is a business entity subject to dominant influence of public law entities. The request concerned two sets of information from the contracts that the insurance company concluded with four business entities: information on contract value and the type of service agreed upon. The Commissioner established that the requested information concerns data that is deemed absolutely public information according to the APIA, i.e. there is no exception applicable with regard to this information. The APIA stipulates that notwithstanding any exceptions from free access to public information, business entities subject to dominant influence of entities of public law must enable access to information on: the type of transaction; a contracting partner which is a legal entity (business name, business address and account of a legal entity) or a natural person (the name and place of residence); contractual value and amount of individual payments; and the date and term of the transaction. As the requested information is absolutely public, the Commissioner ordered the insurance company subject to dominant influence to provide the applicant with the requested information.

Business secret (No. 090-103/2014/6 of 15 July 2014)

The applicant, a journalist, requested access to the minutes of board meetings of the Bank Asset Management Company where the board members discussed the selection of external consultants. The authority refused access to minutes claiming the protection of business secret. However, the Information Commissioner concluded that those parts of the minutes where the selection of external consultants had been discussed do not contain any information that could be considered as business secret. In particular, the Commissioner found no indications that revealing the requested information would result in significant damage for the business of the authority (i.e. the objective criterion for establishing the exception of business secret). Consequently, the Commissioner ordered the authority to provide the journalist with the requested minutes of board meetings.

Classified information, Internal operations of a public authority (No. 090-231/2014/7 of 21 October 2014)

The Government of the Republic of Slovenia rejected the applicant's request for access to the transcript of the 69th regular session of the Government. The Government relied upon the exception of "internal functioning" of the authority, claiming that releasing of the transcripts would cause harm to its internal functioning and operations. The Commissioner found that the transcripts are marked as classified, but this has not been done properly in accordance with the Classified Information Act. Namely, the document was not classified

as soon as it was created and the written assessment of damage - a predisposition required under the Classified Information Act - did not properly specify what kind of damage could arise from providing the document to the public. The transcript cannot therefore be considered as classified and the exception of "internal functioning" is also not applicable as the harm to the functioning of the Government that would be caused by the release of the transcript was not proven. The Commissioner therefore demanded that the authority declassifies the transcript and provides it to the requester.

Classified information, Public interest test (No. 090-164/2014 of 21 November 2014)

The applicant requested from the Police the information regarding the use of IMSI catchers, specifically the information on: the producer; specification; the cost of training, maintenance and repairs; the person responsible who approved the purchase; the type of procedure that led to the selection of the product; the applications (bids) competing for the business deal; total annual usage of the device and annual usage of the device per specific criminal offences. The authority refused the request relying on the exception of classified information and the protection of internal functioning of the authority. The Commissioner decided to partially uphold the requester's appeal against the refusal. Namely, in part that relates to the technical specification, maintenance costs, the person responsible, the type of selection procedure and the applications / bids, the Commissioner set aside the first-instance decision and returned the case back to the first instance. The major criticism on the part of the Commissioner against the first instance decision was that authority failed to consider the right to access of each document individually, but it refused access in general. Moreover, the authority failed to consider whether partial access to documents is possible. In the remaining part, as concerns the statistical information on the annual usage of IMSI catchers, the Commissioner recognised that this information is properly classified, but that the public interest in the disclosure prevails.

Environmental information (No. 090-263/2014 of 28 November 2014)

The applicant requested from a municipality access to the noise impact assessment study, produced by the regional Institute of Public Health, which researched the impact of noise on the environment and health of the local residents. The authority refused the access claiming that the document was in the process of being drawn up, still under consultation and that the disclosure of the document would lead to misunderstanding of its contents. However, the Commissioner found that the exception relied upon by the authority is not applicable, as the document is not still being drawn up, but it is finished, it has been signed by all responsible persons at the Institute of Public Health and sent to the authority. The Commissioner also emphasised that in any event, the information on the effects of noise on the health of the local population is in the public interest. The public interest is especially strong when it relates to issues of public health, environment impact assessments and public spending; the authorities must be even more transparent when it comes to information about these issues.

2.3 General Assessment and Recommendations in the Field of Access to Public Information

In 2014, the number of appeals against decisions refusing requests (i.e. 320) rose comparing to 2013 when the Information Commissioner received 271 such appeals. On the other hand, the number of appeals against administrative silence declined from 339 in 2013 to 258 in 2014. The Commissioner estimates that the fall in the number of appeals against administrative silence of the public sector bodies is a positive sign showing greater responsiveness of the first instance bodies. The increase in the number of appeals against refusals can be ascribed the Amendment APIA-C which brought about the expansion of the bodies liable under the act. This also increased the workload of the Information Commissioner, who noted in practice that the „new" liable bodies (business entities subject to dominant influence) are not fully aware of their obligations and/or dispute these obligations. Such contestation results in the majority of Commissioner's decisions being challenged before the Administrative Court. As the Amendment C only came into force in April 2014, none of these court proceedings had been concluded by the end of 2014.

The Information Commissioner noted in 2014 an increase in the number of appeals against decisions of those „traditional" bodies that concurrently fit into the category of the „new" bodies. Such is the example of the Bank Asset Management Company and some public enterprises. All provisions of APIA are applicable to these bodies in parts of their operations in which they execute public powers or perform public services. The information emerging from the rest of their operations (i.e. in purely commercial parts) still fall within the scope of the APIA, but only to the extent as it is applicable to business entities subject to dominant influence. Thus, these „mixed" bodies should respect the provision on issuing a formal, administrative decision in case of a refusal of the right of access to documents.

The Commissioner estimates that the level of awareness of the right to access public information on the part of requesters is satisfactory, but the bodies liable under APIA still lack knowledge of their duties, especially when it comes to municipalities, bodies of the broader public sector (such as public health and educational institutes and other entities of public law), private bodies exercising public powers and public service contractors. Low levels of awareness of public bodies of their duties under APIA and especially of the new obligations established by the Amendment APIA-C increase the need for promotional and awareness-raising activities in the field. The Information Commissioner, to the extent permissible for an appeal body, thus continued with its practice of promoting the right to information by conducting several workshops and lectures free of charge. In cooperation with the Ministry of Public Administration, the Information Commissioner issued a publication for business entities subject to dominant influence about their new obligations under APIA-C.

As in previous years, the Information Commissioner again draws attention to the issue of charging fees for the work of public officials related to providing public information. The Commissioner believes that the fees for accessing documents should be kept at the lowest possible rate and should not cause a disproportionate obstacle for exercising the constitutionally protected right to access public information. The APIA clearly states that consultation of the information on the spot shall be free of charge and that only material costs may be charged for the transmission of a transcript, copy or electronic record. Nevertheless, some bodies charge the costs for the work of public officials. Such a practice is all too often arbitrary and leaves the Commissioner with no possibility to test in the appeal procedure whether the amount of work claimed to be done is reasonable; this depends on the speed of work of public officials, the organisation of work and the (in)efficiency of record management. The Amendment APIA-C obliged the Government of Slovenia to prescribe, on the basis of the ex ante opinion of the Commissioner, common charging rules for the costs of transmitting the information latest until mid-October 2014. However, the Commissioner has not been asked to review any proposals in this regard and it therefore calls upon the Ministry of Public Administration and the Government to immediately com-

mence with the preparation of a reasonable solution for charging the costs in the form of the common charging rules.

In 2014, the Information Commissioner received eight appeals in regard to the re-use of public information, which is two more comparing to the previous year. This still indicates applicants' poor awareness of the legal mechanisms available to them if their request is not granted. The re-use of public information has important economic potential which remains underexploited in practice. In the area of international cooperation in the field of re-use, the Information Commissioner participated in the international consortium within the LAPSI project (Legal Aspects of Public Sector Information), which concluded at the end of the year.

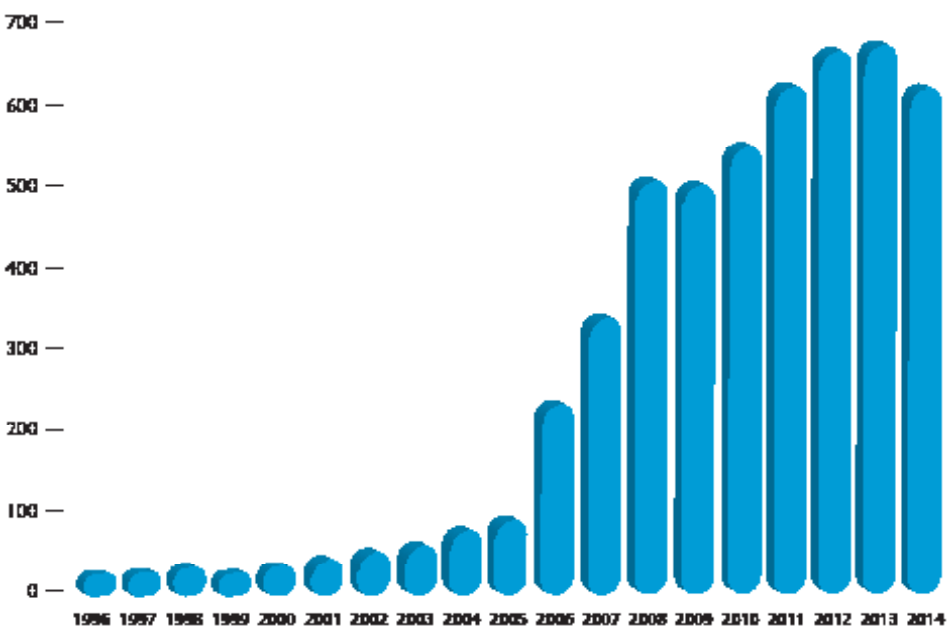
3 WORK IN THE FIELD OF PERSONAL DATA PROTECTION

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[1] provides that the protection of personal data shall be guaranteed, and 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 Personal Data Protection Act (PDPA) of the Republic of Slovenia was adopted in mid-2004, and entered into force in January 2005. The amended Personal Data Protection Act (hereinafter the PDPA-1[2] was adopted in July 2007. The purpose of the PDPA-1 is to define in a uniform manner the rights, obligations, principles, and measures by means of which unconstitutional, illegal, and unjustified interferences with the privacy and dignity of individuals in the processing of personal data are to be prevented. All other (sectoral) laws must be in line with these principles, and must clearly determine which personal data processing systems are to be established, which specific types of personal data they are to contain, the purpose of processing the collected personal data, and any possible limitations of the rights of individuals. Furthermore, data processers relying on the data subject's consent or other legal grounds are also bound by these principles. Finally, in Part VI, the PDPA-1 is also a type of a sectoral act, defining the obligations of data controllers in the fields of direct marketing, video surveillance, biometrics, building access controls, as well as professional supervision.

The enforcement of the PDPA-1 is entrusted to the office of the Information Commissioner. In doing so, the Information Commissioner in 2014 conducted a total of 628 inspections of suspected violations of the act; 206 in the public sector and 422 in the private sector. Most of the inspections were initiated upon receiving a complaint (194 and 410, respectively), while the rest were initiated ex officio (11 and 12, respectively) and in accordance with the annual inspection plan. It should be noted that the total annual number of inspections is somewhat lower than the year before, but this is mainly attributed to the lower number of complaints received (722 in 2014 compared to 852 in 2013).

Figure 4: The number of cases that the Information Commissioner conducted on the basis of suspected violations of PDPA-1 provisions between 1996 and 2014.



1 Official Gazette RS, Nos. 33/91-I, 42/97, 66/2000 and 24/03. An unofficial English transation may be obtained on the Website of the Constitution Court of the Republic of Slovenia, http://www.us-rs.si/en/about-the-court/legal-basis/

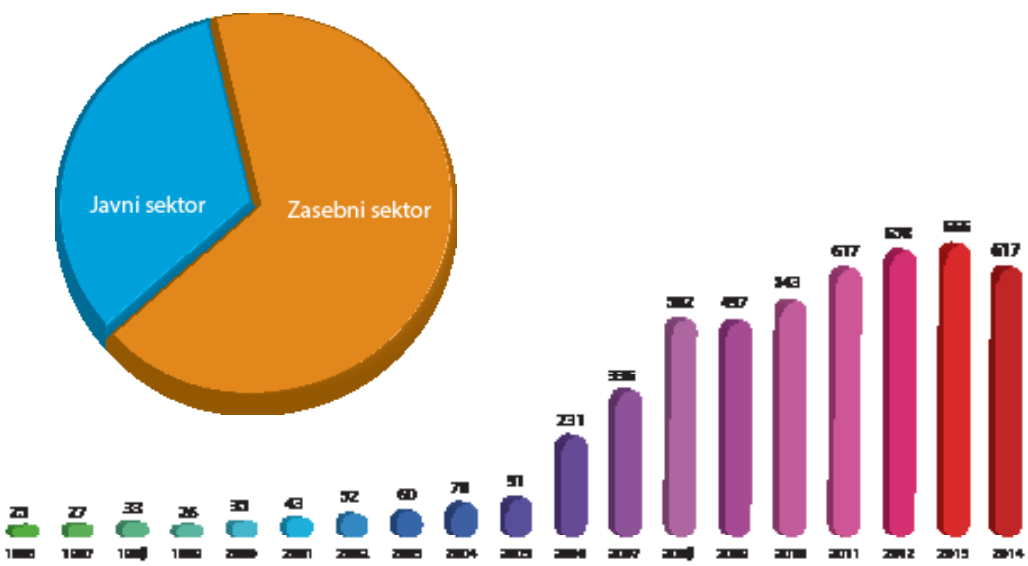
2 Official Gazette RS, No. 86/2004; hereinafter: the PDPA-1.

Within the framework of the above inspection procedures, 47 on-site inspections were carried out in the public sector and 97 in the private sector. Additionally, 32 inspections of websites were carried out, mostly in relation to the oversight of the provisions on cookies and similar technologies. In order to address the established irregularities, the state supervisors issued a total of 67 warnings and 26 regulatory or administrative decisions.

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

- unlawful disclosure of personal data; the transfer of personal data to unauthorised users by data controllers and unlawful publication of personal data (182 cases);
- unlawfully collecting or requiring personal data (127 cases);
- abuse of personal data for direct marketing purposes (91 cases);
- unlawful video surveillance (73 cases);
- inadequate security of personal data (33 cases);
- other (123 cases).

Figure 5: Complaints regarding unlawful processing of personal data from 2006 to 2014, a comparison between the public and the private sectors.

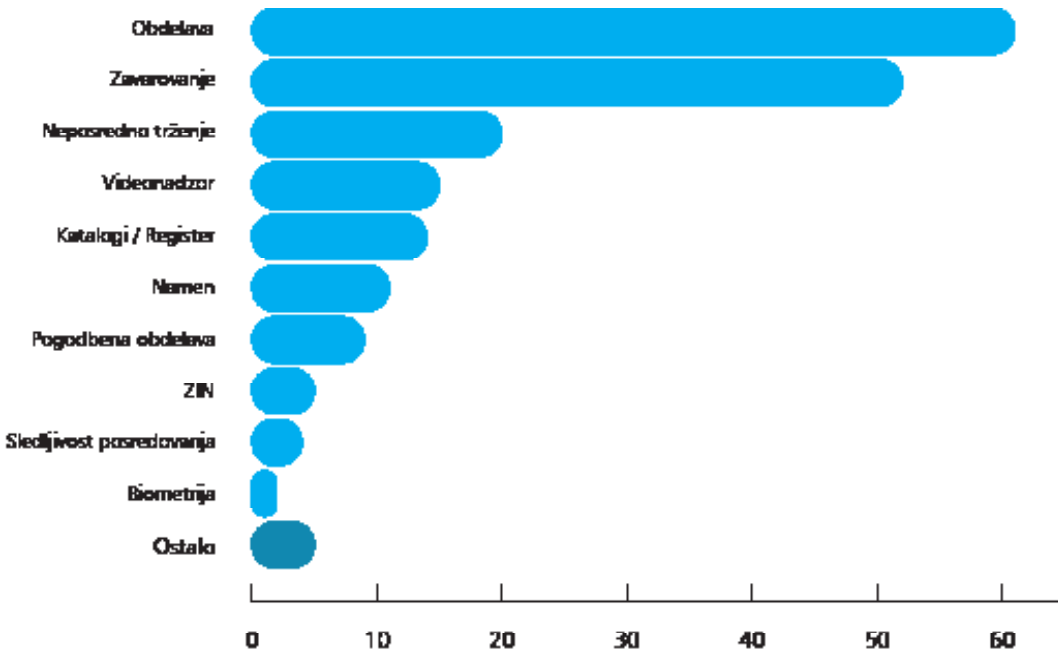


In addition, a total of 95 offence procedures were initiated in 2014 due to PDPA-1 violations, of which 22 were against public sector legal entities, 52 against private sector legal entities, and 21 against individuals. In those procedures the Information Commissioner issued 19 warnings and rendered 76 decisions (26 cautions and 50 fines). Furthermore, the Information Commissioner issued 55 additional warnings for minor violations. In response, the suspected offenders filed a total of 10 requests for judicial protection.

In 2014, the Information Commissioner received a total of 19 court decisions pertaining to this and past year's decisions, with 7 of those ending with a reduced fine, 5 annulling the Commissioner's decision, and 7 being dismissed either on formal of material grounds.

In 2014, the Information Commissioner received a total of 2,040 requests to issue a written opinion in relation to specific questions. It issued 49 fully-written opinions and explanations, and in 1991 cases it referred applicants to opinions already issued. Most opinions are published on the following website: www.ip-rs.si. The Information Commissioner issued additional opinions and explanations orally. Every working day between 9 am and 3.30 pm there is a state supervisor on duty at the office who can answer questions over the telephone.

Figure 6: The most common violations of PDPA-1 provisions in 2014.



In 2014, 9 decisions were issued on the permissibility of implementing biometric measures, and 4 new applications were received. The Information Commissioner fully granted the request from a government agency to employ fingerprint and retina scanners to secure access to dedicated premises holding secret and top secret government and EU/NATO documents. It also partially granted requests by 4 connected companies to employ fingerprint scanners in their joint offices, while restricting their use to server room facilities and chairman offices and to select employees authorized to use those facilities, and rejecting use at the main entrance to the office building, entrances to the manufacturing hall, wardrobe facilities, and other spaces where their use could either not be justified or was not proven to be sufficiently effective. The Information Commissioner also rejected the request from 4 applicants who wanted to use biometric measures for less justified purposes, i.e. to monitor employee working hours or to secure access to elevators, parking facilities, and other non-critical office space, because their applications were too widely framed, and because a similar results could have been achieved using conventional and much less invasive security methods.

In 2014, the Information Commissioner received 11 new applications for the transfer of personal data outside the Republic of Slovenia. It issued a total of 13 decisions (2 to requests from the year before), all them positive, permitting the transfer of employee data to the parent companies of several pharmaceuticals companies and importers, use of US cloud based email and human resources software to a steal manufactures, and exporting of client data to several business consulting firms, a cosmetics firm, an IT firm, and several medical and laboratory supply and equipment importers. It did not issue any new country adequacy decisions.

In 2014, the Information Commissioner granted permission to 9 data controllers to link with another or other personal data filing systems. It permitted the linking of filing systems to the following institutions: the Pension and Disability Insurance Institute of Slovenia (ZPIZ) and the Agency of the Republic of Slovenia for Public Legal Records and Related Services (AJPES) for ZPIS to receive employer updates from AJPES'es Slovenian Business Register (PRS) based on the employee's personal registration number (EMŠO), the Public Guarantee, Maintenance and Disability Fund of the Republic of Slovenia and the Ministry of the Interior (MNZ) to receive beneficiary information from MNZ's Central population register (CRP), also based on the EMŠO; the High Court and the State financial authority (FURS) to link the court's electronic enforcement system with the state VAT registry based on the individual's VAT number; the Health Insurance Institute of Slovenia and the State financial authority (FURS) to link their

central register of beneficiaries with the FURS VAT register and accounting reports register, again based on the individuals VAT number; the Ministry of Justice to link their Register of expert witnesses, appraisers and translators with the Central Population Register (CRP) with the Ministry of Interior (MNZ); The Ministry of Education, Science and Sport to link their Registry and analytical system for higher education with enrolment data of several public universities, based on the student's personal registration number (EMŠO), as well as their own enrolment registry, also based on the EMŠO; the Pension and Disability Insurance Institute of Slovenia (ZPIZ) to link with the above mentioned Registry and analytical system for higher education with the Ministry, again based on the EMŠO, finally, the Ministry of Justice (MP) and the State penal authority (ZIKŠ) to link inmate data with the MNZ's Central Population Register (CRP), also based on EMŠO.

In 2014, the Information Commissioner received 72 appeals regarding the right to access to one's personal data. The appeals mostly concerned state authorities, ministries, and constituent bodies (39 cases, 58%), with the rest about evenly split between health care institutions, insurance companies, telecommunications operators, banks, courts, municipalities and other data controllers. In 19 cases data controllers enabled individuals access to requested data upon being called on to do so, while 4 data controllers were ordered by a decision to do so. 14 applicants were advised how to act, while 3 withdrew their appeals. The Information Commissioner transferred 8 appeals to competent authorities for consideration, in 1 case it issued a decision rejecting the appeal on the grounds that the application was incomplete or had been submitted prematurely, and in 2 cases it issued a decision dismissing the appeal.

In 2014, the Information Commissioner did not file any requests for a review of the constitutionality to the Constitutional Court of the RS.

In July 2014, the Constitutional Court repealed certain articles of the Electronic Communications Act that enacted disproportionate intrusion into everyone's privacy by imposing mandatory data retention for a prolonged time. In 2013, the Commissioner requested that the Constitutional Court reviews the constitutionality of the Electronic Communications Act. The Court stayed the proceedings until the preliminary question, referred to the European Court of Justice with regard to the Data Retention Directive, is settled. Following the judgment of the ECJ in joint cases C-293/12 and C-594/12, the Constitutional Court declared the data retention regime set by the Electronic Communications Act unconstitutional.

3.2 Selected Cases Involving a Violation of Personal Data Protection

E-mail address database trading

Information Commissioner received a complaint which pointed to a data controller offering a database consisting of roughly 40,000 e-mails for sale on the internet. The question was whether the individuals, whose e-mails were in the database, have consented to their e-mail being part of the database and intended for sale. The data controller explained that it acquired the e-mails through its own telephone studio and through its clients. The individuals have supposedly given their consent orally and have agreed to being sent the first commercial message. The data controller further argued that the database included only e-mail that have previously been made public in the online business register BIZI where the individuals entered indeed gave permission to be sent the first commercial e-mail.

The Information Commissioner held that the data controller must erase all emails of natural persons from the database, since it has not proved that the individuals consented to their e-mails being processed this way. The Information Commissioner further reasoned that the publication of e-mails online does not by itself constitutes a legal basis for those e-mail being included in a new data filling system. The legal basis for establishing a new database must be in accordance with Article 10 of the PDPA-1, namely be based on the consent of the individuals.

E-mail redirection after termination of employment contract

The Information Commissioner fined a university and its responsible person for IT matters because an e-mail address of a former employee of the university (in the form name.surname@universityname.si) was redirected to a general info e-mail address of the university, after he has already terminated the employment contract.

The Information Commissioner found that the university and the responsible person for IT matters had no legal basis for such personal data processing, since there was neither a legal basis in the law, nor has the individual consented to his e-mail being used after the termination of his employment contract with the university. Additionally, it was established that through the redirection of the e-mail address the persons that has access to the general e-mail address (the IT person and the secretary) unlawfully obtained access to additional personal data of the concerned individual, namely the identification of senders of e-mails and time of the communications. The Information Commissioner held that such redirection was not necessary for the continuity of the work of the university since there are other means available in cases when a person terminates an employment contact, but his/her work needs to be continued by other persons, for example by blocking of e-mail address and setting up an auto-reply with new contact details, a measure commonly used in practice. Regarding the question of consent to such personal data processing being given in the employment contract, the Information Commissioner emphasised that for such consent to be valid it would have to be freely given and respect the principle of proportionality, and would have to be given at the time of employment contract termination not in the contract itself.

Identification of individuals, allegedly having not paid for parking tickets while on holiday in the neighbouring country of Croatia, based on licence plates numbers

Information Commissioner initiated an inspection procedure against a law firm based in Slovenia that was acquiring personal data of Slovenian citizens that have allegedly not paid parking tickets in two coastal towns in Croatia, authorised by two Croatian firms issuing parking tickets. The law firm firstly acquired identification data of Slovenian citizens, based on the registration plate number provided by the two firms issuing parking tickets, from different administrative unites in Slovenia that have access to the registered vehicles records. Upon identification of the registration plate number holders, the law firm sent the individuals a reminder before the enforcement, requesting them to pay the allegedly outstanding parking ticket fee and, additionally, the costs of the reminder. The law firm attached to the reminder a list of other registered plates numbers that were allegedly also in debt to the firms issuing parking tickets.

The Information Commissioner considered two issues: (1) whether the law firm had legal basis to acquire identification of the holders of the registered plates numbers and (2) whether the law firm had legal basis to disclose the licence plate numbers of all other alleged debtors to the alleged debtor in the reminder. Regarding the first question, the Information Commissioner found that the law firm had legal basis for identification in the Attorneys Act, since the request to the administrative unites was made as part of a civil law matter in a case concerning a creditor and a debtor, and not as part of the criminal law procedure. To acquire the information free of charge in such cases the law firm needs to present the power of attorney and explain why such information is necessary in a given case. Regarding the second issue, the Information Commissioner found that the law firm had no legal basis for disclosure of the registered licence plate numbers (which constitute personal data) to all recipients of the reminder.

Video surveillance of the entrance to a landscape park

A landscape park was ordered to stop video surveillance of the entrance to the park that involved three video surveillance cameras, located on a street lamp. The notification of the

video surveillance was located at the reception building. The first camera was covering the access area to the entrance, the second was covering the reception and the persons collecting the entrance fee, and the third was monitoring the area in front of the entrance where drivers stop to pay the fee. The purpose of the video surveillance, as explained by the landscape park operator, was to control the traffic and the collection of the entrance fee, to record the traffic in the season when fees are not charged, to provide live information about weather conditions to the Environmental Agency of Slovenia, and for tourism purposes.

The Information Commissioner found that these purposes could have been fulfilled with milder means, not encroaching on the privacy of the visitors of the landscape park. Video surveillance is only allowed in cases when the protection of property or safety of the persons needs to be ensured, which was not the case for the three mentioned cameras. Additionally, the Information Commissioner held that the operator of the landscape park did not execute any of its lawful interests by video surveillance, since it could fulfil all the purposes specified above by milder means, not including monitoring individuals. Video surveillance for monitoring employees is also not allowed. If video surveillance is used as a means to protect the property, it has to be located in a way to monitor the property and not the entrance point to the park in general.

Video surveillance in a retirement home

An inspection by the Information Commissioner revealed that a proprietor of a private retirement home conducted video surveillance throughout the property, including all common rooms available to the patrons (but not their private rooms) and all the rooms of the adjacent fitness and bar facilities which were also available to the patrons. The justification provided by the proprietor was that the all-out surveillance was necessary to prevent physical attacks and/or theft against the patrons, to "ensure the good behaviour of the staff", and to better monitor the workflow in the kitchen and some other areas of the retirement home.

This was found to be in breach of Articles 75 and 77 of the PDPA-1, which allows video surveillance of workplace entrances only when required to protect life and property, and limiting surveillance of workplace innards to even stricter standards. As a consequence, the placement of most of the video cameras (those in the common areas) was found to be unlawful, and the proprietor was immediately ordered to remove them. A subsequent analysis showed that the rest of the cameras had to be removed as well, because even though they were placed in areas that could be considered more sensitive and that thus could have justified the need for video surveillance, the proprietor had not gone through a proper process to identify those areas as sensitive. The entire video surveillance setup was thus deemed as unlawful under the PDPA-1.

The proprietor challenged the decision in court, but was ultimately rejected.

Information about unpaid school meals in school kitchen

A school introduced a new system for managing the subscriptions to school meals. It included a monitor which showed the name and surname of a pupil and the data on the number of paid meals and the data on unpaid services. A beep warning was in place when a pupil with unpaid services approached, and this way the information about the unpaid services was disclosed to unauthorised persons in the school kitchen.

Upon the Information Commissioner's warning, the school disabled the monitor and the warning beep in the computer programme, and thus disabled the disclosure of data from the records of school meals in the school kitchen. The school cook was only authorised to process data on the pupils that require dietary specificities.

Collection of employee data for HR analysis purposes

The Information Commissioner received a complaint alleging that an employer was unduly collecting very detailed and possibly sensitive personal data (i.e. on whether the employee is a single parent or a 2nd generation worker).

During the inspection visit, it was determined that the data was being collected as part of an extensive written employee survey done for human resource (HR) management purposes. The survey had already been completed, but the answers were still being stored in paper form in the employees' personnel folders. The Commissioner also determined that the survey was accompanied by a statement to be signed by the employee, stating that the he/she is submitting the answers voluntarily.

Subsequent analysis of the supporting documents revealed that while the employer did indeed have a legal basis for collecting the data (it was needed for managing the workforce, which forms a valid legal basis under Article 48(1) of the Employment Relationship Act), it did not properly inform the employees about who the data controller was, what the purpose of the collection was (it was too broad and vague) and whether participation was indeed voluntary or not. This was found to form a breach of the data controller's obligation to inform the data subjects (Article 19 of the PDPA-1), thus rendering the subsequent data processing unlawful. The employer was thus ordered to destroy the collected surveys and statements, which it did voluntarily.

3.3 General Assessment of the Status of Personal Data Protection and Recommendations

In 2014, the Information Commissioner conducted 628 inspections in the field of data protection, of which 206 pertained to the public sector and 422 to the private sector (712 in 2013, 725 in 2012, 682 in 2011, and 599 cases in 2010). At the same time, 95 minor offence procedures were initiated due to PDPA-1 violations (106 in 2013, 158 in 2012, 136 in 2011, and 179 in 2010).

Aside from inspections and offence procedures, in 2014, the Information Commissioner received 2,040 requests to issue a written explanation or an opinion in relation to specific questions (2,460 in 2013 and 2,191 in 2012, 2,143 in 2011, and 1,856 in 2010), 14 requests for a decision on the permissibility of linking personal data sets (6 in 2013, 9 in 2012, 14 in 2011, and 9 in 2010), 4 requests for a decision on the permissibility of implementing biometric measures (6 in 2013, 9 in 2012, 9 in 2011, and 6 in 2010), 11 requests for authorisation of a transfer of personal data to third countries (14 in 2013, 5 in 2012, 4 in 2011 and 8 in 2010), and 67 appeals regarding the right to access one's personal data (68 in 2013, 63 in 2012, and 85 in 2011 and 2010, respectively).

The statistics show that the number of complaint-based inspections has gradually started to level off; and for this reason the Information Commissioner has decided to increase the number of ex officio inspections per data protection supervisor from 1 to 3 annually, particularly targeting the biggest data processors in the government, municipalities, health, personal loan, defence and police sectors. The results of these ex officio inspections show that there no major violations had been found. The violations that had been discovered mainly related to the insufficiently thorough procedures and measures prescribed for the protection of personal data or inconsistent exercise of such measures and procedures.

In 2014, as in the previous years, the highest number of complaints received by the Information Commissioner concerned unlawful disclosure or publication of personal data (182), the majority of which related to the publication of personal data on social networking

sites (mainly Facebook). As a rule, the Information Commissioner is not competent to take action in such cases as personal data published online had not been taken from a filing system. This, however, does not mean that the concerned individual is stripped of any legal protection; he/she has the recourse to courts to protect his/her rights under the Code of Obligations or the Criminal Code.

A large number of complaints related to the issue of direct marketing (91 in total). The violations found by the Commissioner related mainly to the issues of unlawful obtaining and the use of personal data; not informing the individuals of their right to opt-out; and not respecting the opt-out notice. Among the frequent violations observed are still those regarding unlawful disclosure of the e-mail addresses of the recipients of a message in the "To" or "Cc" fields when such addresses should have been entered in the "Bcc" field.

Among cases related to video surveillance (73 in total), most of the irregularities found pertained to the use of video surveillance cameras in places where the PDPA-1 does not allow them to be used, in particular public places and/or work places where the setting of cameras cannot be properly justified. There were also several cases where access to the recording device was not properly secured and logged, and cases of insufficient information given to the individuals on the use of video surveillance.

In numerous complaints received by the Commissioner, the complainants claimed that different bodies obtained their personal data for the purposes of conducting official proceedings (e.g. for offence procedures) unlawfully or they claimed that the bodies obtained personal data that they did not need for specific proceedings. In relation to that, the Information Commissioner explained that it is not competent to initiate action to ascertain whether an authorised person of an official body acted and decided lawfully in a specific case under its jurisdiction. Doing so would mean overstepping its competencies as established by a recent Constitutional Court ruling.[3] The Court reasoned that such claims of supposedly unlawfully obtained evidence are to be resolved in that very procedure or during subsequent judicial redress, and not through the Commissioner.

In regard to the workplace privacy, the Information Commissioner received several complaints regarding supposed redirecting and/or monitoring of employee e-mail, especially after the termination of the employee's contract. This problem had already been noted in the last year's report, but some employers have still not abandoned such practices. This, the Information Commissioner issued a special press release in the beginning of September. The Commissioner believes that such practices are a result of vague regulations in this field and has in the past suggested several times that the authorities adopt a law that would regulate the issue of workplace privacy comprehensively. A few years ago, the Commissioner even sent its proposal of the Workplace Privacy Bill to a competent Ministry, but due to the lack of political will the area is still not properly regulated.

Finally, in regard to e-privacy in the use of cookies by Slovenian websites, the number of complains continues to decline (down to 15 from 50 in 2013). However, the required workload (due to the need to inspect upwards of up to 200 websites, some significantly large) continues to be considerate. The Information Commissioner was thus forced to handle the individual complaints according to priority and available resources, but was still able to conclude a total of 52 inspections by the end of 2014. In all cases, the website owners were prepared to modify their cookie policy accordingly, clarifying their use of cookies and offering meaningful choice regarding the use of advertising and other invasive cookies. We thus view the regulatory situation regarding cookies as effective, and strive to continue that trend in 2015.

Preparation and publication of new guidelines also continues to be an important goal of the Information Commissioner. In 2014, the following guidelines were issued:

- Guidelines for data protection when using GPS devices;
- Guidelines for data protection for internal marketing surveys;
- Privacy Impact Assessment (PIA) guidelines for the introduction of new police powers.

3 No. U-I-92/12-13, 10.10.2013

The GPS guidelines were prepared as a response to a growing number of questions regarding the use of global positioning technology in various aspects of business and private life, even when the proportionality of that use may not always be apparent, i.e. regarding its use in taxis and employee-issued vehicles, tracking of parking enforcement officers, newspaper delivery crews, and patrons in retirement facilities. In the guidelines, the Information Commissioner clarified its position on the requirements the technology, and the required minimization and security provisions to be put in place.

The internal marking survey guidelines were prepared in cooperation with the competent industry body, and guide the users through the process (and necessity) of obtaining consent and other requirements when conducting user surveys among loyalty club members and other similar consumer relationship management (CRM) scenarios.

Particular focus went into the preparation of the Privacy Impact Assessment (PIA) guidelines for the introduction of new Police Powers (also available in English translation at https://www.ip-rs.si/index.php?id=388), which provide a comprehensive framework for cautious, well-thought-out and legitimate introduction of new police powers, with particular focus on those with a strong technological aspect. The Criminal Procedure Act of Slovenia (the ZKP) has had its fair share of amendments over the last 20 years, and has thus had many new police powers added. Unfortunately, not all of those proposals were accompanied by an adequate expert discussion. Consequentially, the usage of new powers has been riddled with difficulties, often subjected to exclusion of evidence before the courts of law, and sometimes met with outright dissent by both the general as well as professional public. To help with these issues, the guidelines lay out a comprehensive framework for conducting a pre-emptive Privacy Impact Assessment (PIA) of new legislative proposals dealing with police powers. The feedback that the Information Commissioner received made us confident that the Guidelines are an important and useful tool for all concerned parties and we are delighted to note that high ranking representatives of the Director General of the Police publicly committed themselves to the use of the Guidelines.

Another important trend the Information Commissioner has closely observed in 2014 is the development of "big data" applications, such as the use of connected ("smart") electric and gas meters, the proliferation of smart TVs, mobile "black boxes" linked to insurance and toll collection providers, and so on. Vast databases that allow for quick collection and processing of various (non)structured data sources make it possible to "see" and "measure" things that were not possible before. With the parallel emergence of "Internet of Things" where the device can collect more and more data in a digital format, the amount of personal data collected on individuals experiences and unprecedented increase. The amount of information controlled by the data controller using such technology is so great that it allows for identification of business trends, shopping habits, traffic patterns, all the way to forecasting outbreaks of flu and the likelihood of crime in a given geographical area. As well as the (correct or incorrect) inferences and conclusions about an individual's credit rating, health, shopping habits and other characteristics - data that could have not been infered previously. Implications for the protection of personal data can be large, that is why "big data" is certainly among the most important new phenomena whose development should be monitored with utmost care, when it comes to question of privacy.

Finally, the use of drones and the sensory devices they may carry has been an area of particular interest in 2014. Drone use has increased greatly in 2014, and while offering many legitimate uses (disaster recovery, measurement, media coverage, aiding police and other government forces), they also present significant data protection challenges, particularly those related to covert and dragnet (government) aerial surveillance using their wide array of sensors. In order to systemically approach this field, the Information Commissioner has reached out to the national Civil Aviation Agency (CAA) and the competent Ministry of the Environment and Spatial Planning to prepare national guidelines for drones use, but was yet to receive a response.

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

In 2014, the Information Commissioner again noted a worryingly high 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 protecion.

Some of the acts and regulations that the Commissioner commented on in 2014 include:

- The Draft Act Amending Electronic Commerce Market Act;
- The Draft Act Amending the Consumer Protection Act;
- The Draft Act Amending the Criminal Procedure Act;
- The Draft Act Amending the Political Parties Act;
- The Draft Act Amending the Referendum and Popular Initiative Act;
- The Draft Act Amending the Gaming Act;
- The proposal of the Removal and Transplantation of Human Body Parts for the Purposes of Medical Treatment Act;
- The Draft Banking Act;
- Several proposed international agreements for police cooperation.

4.2 Relations with the Public

Throughout 2014, the Information Commissioner provided for the public nature of its work through its website www.ip-rs.si and it raised the 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). It endeavoured to ensure that its website was up to date and comprehensive. The majority of information on its website is also available in English. By organising a variety of workshops and seminars it provided for the continuing education of liable entities and persons; 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, whose mandate is to create a safe and open internet environment for children.

The Information Commissioner also marked European Personal Data Protection Day (28 January) and organised an event on the topic of surveillance of intelligence services in the light of revelations of mass surveillance by Edward Snowden. At the event, the Commissioner, now traditionally, also awards a best practice award in the area of personal data protection. In 2014, Kreditni biro SISBON was awarded for efforts in the field of data protection as established in the inspection procedure led by the Commissioner. Furthermore, awards were given to companies that in 2013 entered a certification scheme ISO/IEC 27000 information security management standard and thus demonstrated a high level of personal data security.

Every year on 28 September the International Right to Know Day is marked. On this occasion organizations from all over the world emphasise the importance of the fight for transparency and accountability of the public sector and of ensuring efficient participation

of citizens. On this occasion, the Information Commissioner held a roundtable where invited speakers discussed the question of whether greater transparency strengthens the rule of law. Hosted by the current Information Commissioner, Mojca Prelesnik, the issue was discussed by the Human Rights Ombudsman, former ministers, a law professor and the representative from civil society and the Information Commissioner of Croatia. On this occasion, the Commissioner awarded the Transparency Ambassador prize for best practice in the field of access to public information to the Ministry of the Interior – the Police.

In 2014, the Information Commissioner continued its prevention activities and dedicated a great deal of attention to disseminating tools and aids for raising awareness. The Commissioner released the following guidelines: Guidelines on protecting personal data during internal market studies; Guidelines on the use of GPS tracking devices and personal data protection; Privacy impact assessment when introducing new police powers. In the field of access to public information, the Information Commissioner in cooperation with the Ministry of Public Administration issued a publication for business entities subject to dominant influence about their new obligations under APIA-C.

At the 7th International Conference of Information Commissioners in October 2011 in Ottawa, Canada, the community of information commissioners and similar institutions ensuring the transparency and protection of the right to access information adopted the decision to create and present to the public a common website of all information commissioners. The website info-commissioners.org was created and managed by the Slovene Information Commissioner also in 2014.

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 2014, the Information Commissioner actively participated in six 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 Technology Subgroup, the Future of Privacy 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 co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of CIS;
- at co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data for the supervision of VIS;
- at co-ordination meetings of the European Data Protection Supervisor (EDPS) together with state national authorities for the protection of personal data (EURODAC).

In 2014, the Information Commissioner Nataša Pirc Musar continued to hold the position of Vice-Chairman of the Europol Joint Supervisory Body until June 2014. In April 2014 a representative of the Commissioner participated in the international inspection group that carried out an inspection regarding personal data protection for Europol at the headquarters in The Hague. The Information Commissioner also regularly participated in the International Working Group on Data Protection in Telecommunications (IWGDPT). Once again in 2014, a representative of the Information Commissioner participated in the Council of Europe's Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

In 2014, the Information Commissioner hosted representatives of similar institutions from a number of countries, such as Bosnia and Herzegovina, Croatia, Albania, Romania, Montenegro and Ukraine to whom it presented its activities and good practices in its fields of competence.

In a consortium with partners from different EU Member States the Information Commissioner started to work on a 3 year project CRISP, which focuses on evaluation and certification schemes for security products. The Information Commissioner is also one of the partners in the European project ARCADES, that centres on inclusion of data protection and privacy protection topics in curriculums of primary and secondary schools in the EU.

In December 2014, the European LAPSI project (Legal Aspects of Public Sector Information) on removing the obstacles to the implementation of the re-use of public sector information concluded. The Information Commissioner has been a member of this project since its beginning in January 2013 and took part in all the project meetings and actively participated in preparing the different project outputs.

Editor:

Mojca Prelesnik, informacijska pooblaščenka

Authors:

Monika Benkovič Krašovec, **Ph.D.** State Supervisor for the Protection of Personal Data
Jože Bogataj, Head of State Supervisors for the Protection of Personal Data
Eva Kalan, State Supervisor for the Protection of Personal Data
Kristina Kotnik Šumah, Deputy Information Commissioner
Maja Lubarda, Advisor
Andrej Tomšič, MA, Deputy Information Commissioner

Design:

Bons d.o.o., Klemen Kraigher Mišič & Matjaž Drev, MA

Photography:

Klemen Kraigher Mišič & Fotolia

Translation

Polona Tepina, LL.M.

The Information Commissioner of the Republic of Slovenia
Zaloška cesta 59
1000 Ljubljana

www.ip-rs.si
gp.ip@ip-rs.si

Ljubljana, May 2015

ISSN 1854-9500