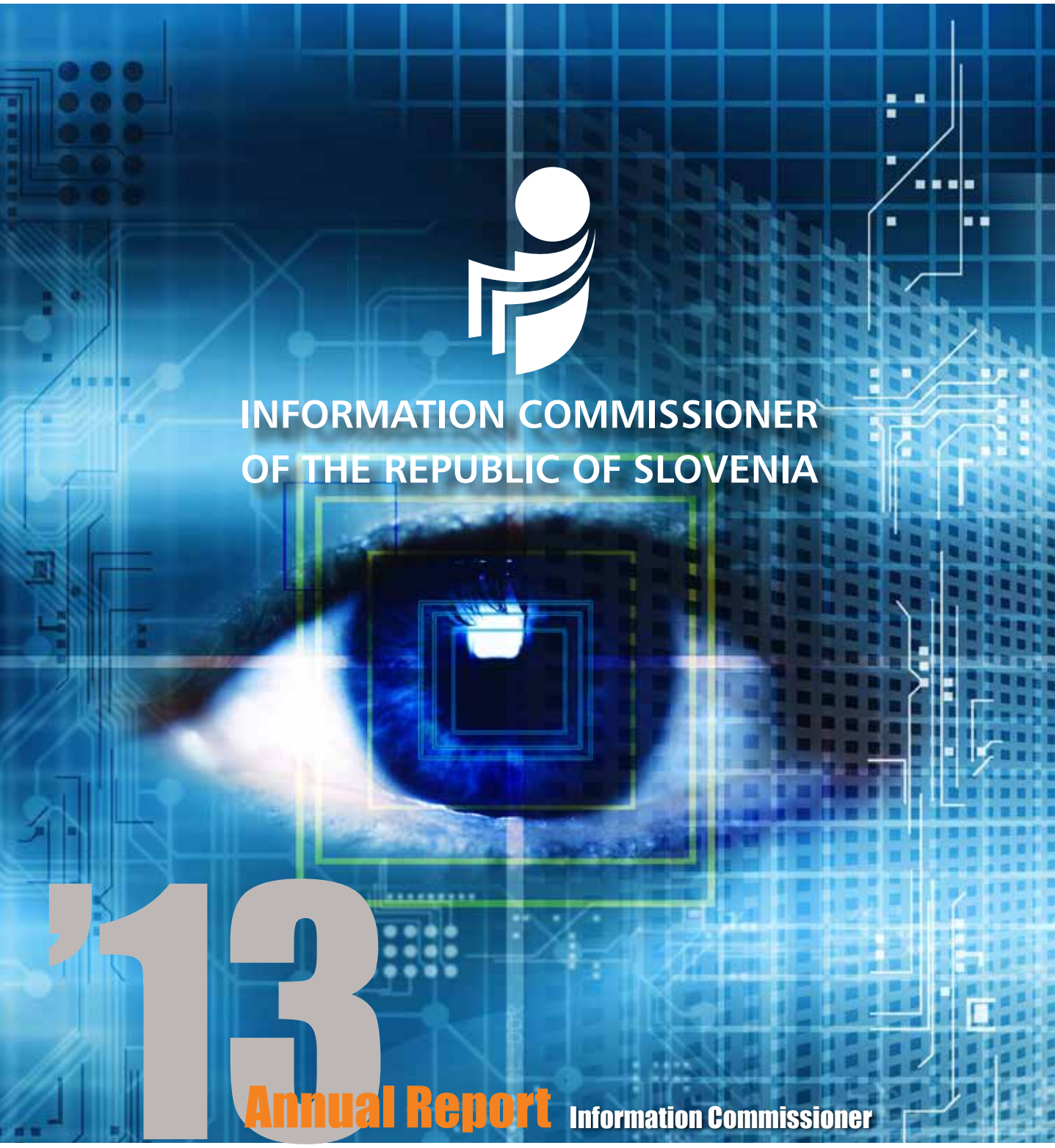
INFORMATION COMMISSIONER OF THE REPUBLIC OF SLOVENIA



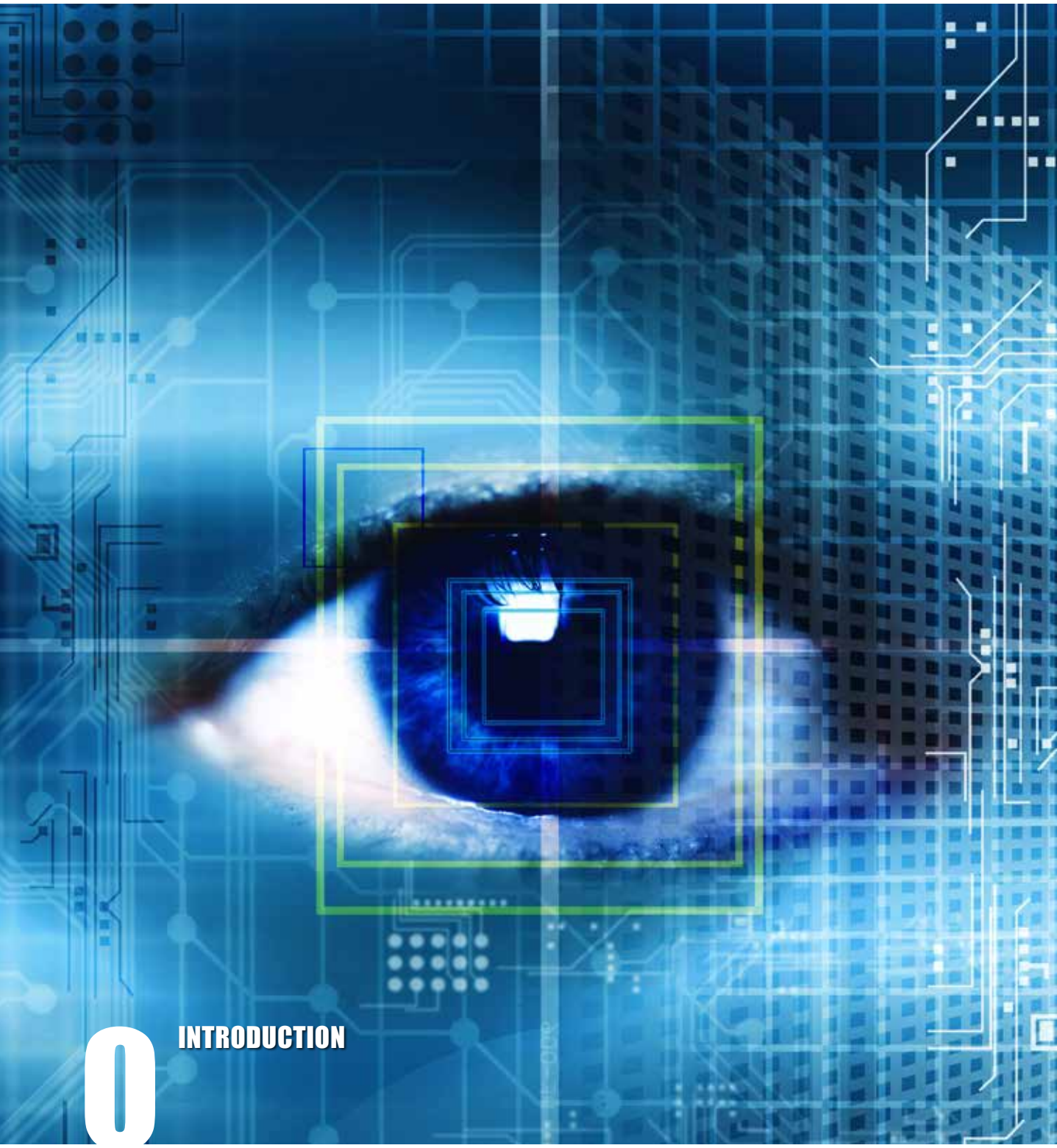
'13 Annual Report Information Commissioner

2013

'13 Annual Report

Information Commissioner

2013



0 INTRODUCTION

2013 marked the tenth anniversary of operation of the Information Commissioner, whose role has grown through these years from one of a small scale appeals body headed by the Commissioner for Access to Public Information, to one as an important guarantor of transparency and the protector of personal data. In 2013 I also completed the last full year of my ten year mandate as the Information Commissioner, a role to which I have devoted two wonderful decades of my life, and which I will always remember with great fondness.

In both fields of its operation the Information Commissioner has once again this past year, received a large (record) number of applications from individuals, covering requests for opinions, complaints and appeals. On the one hand this is gratifying as it clearly indicates that individuals are becoming more and more aware of the purpose and importance of both of the human rights dealt with within the competences of the Commissioner. At the same time we cannot ignore the fact that again in this past year, the marked increase in the number of complaints and inspections carried out can be attributed to the continuing trend of troubling practices by responsible authorities in the area of access to public information, while on the other hand we have the increasingly unmanageable appetites of a wide variety of data controllers, both private and public, eager to gather and process personal data.

2013 brought with it a number of important milestones, which helped us to comprehend just how very much we can lose when we surrender our privacy. Notable incidents, related to invasions of privacy, revealed how major invasions into our privacy occur, in effect, every day, and how powerless we are as individuals if the state loses its control in this area. I was named by the European Commission to participate in a special ad hoc group EU–USA, whose job it was to determine what activities were actually being carried out by the American National Security Agency with regard to the mass gathering of information and personal data of European citizens. At its conclusion I prepared a special report. In the past year we have also taken a major step towards being better able to ensure transparency in the activities of the (Slovenian) state and the public sector in its broadest sense. Preparation of changes to the Access to Public Information Act (ZDIJZ) and the reasons for such change have shown that the state can and must operate much more transparently. Preparation of the last amendment to the Act (ZDIJZ), which came into effect on April 17 this year, and will contribute immensely to greater transparency, is also a result of persistent calls from the Commissioner for greater transparency of the activities of companies that are state-owned, owned by local municipalities or public institutions. In recent years the Commissioner has repeatedly called on those in authority, to turn their words into actions, to ensure greater transparency in the business activities of companies that are state-owned or owned by local municipalities; throughout this period the Commissioner has also actively participated in the preparation of legislative changes.

The Information Commissioner has in this way, on various levels, again played an important role in interceding the paths of detected shortcomings in the structure of society and of the state. In the past ten years the Commissioner has developed into a trustworthy

and respected national appeal body in the field of access to public information as well as a supervisory authority for the protection of personal data. I feel I am able to make such claims given the results of public opinion research, given the responses of people who turn to us for assistance, given the acknowledgement of international colleagues and most importantly given the judgements handed down by the courts, where, in considering appeals lodged against our decisions, in the majority of cases, confirm our position.

The path my colleagues and I have travelled these past ten years has not been an easy one. It has been, however, a path filled with exceptionally interesting challenges, learning, excellent collaboration and many wonderful moments spent with an excellent team of professionals, who are, as I am, concerned each day about how well and effectively two important constitutional rights: the right of access to public information and the right to personal data protection, are being enforced.

Personal data and public information are currencies of the information age, thus the challenges ahead for the new Commissioner, are still considerable. I have no doubt that he or she will, with the support of the excellent team which remains, meet those challenges head-on, and that the Commissioner will continue to carry on their work to the best of their ability, in the best interests of those who govern and for all of us, who live in Slovenia.

Yours sincerely,

Nataša Pirc Musar,
Information Commissioner

INDEX

1 A GROUNDBREAKING TEN YEARS FOR TRANSPARENCY AND PRIVACY – THE ROLE OF THE INFORMATION COMMISSIONER

Russian transparency activist Ivan Pavlov once said:
»Human rights are like muscles, if we don't use them, they wither.«

1.1. The Establishment and Role of the Information Commissioner

The Information Commissioner has been operational since 2003; operating at first as the Commissioner for Access to Public Information, an appeals body dealing with access to public information, with a total of four employees. In 2006, with the adoption of the Information Commissioner Act and the merger of the Commissioner for Access to Public Information with the Inspectorate for Personal Data Protection, the Information Commissioner, as we know it today, was established, with combined competences as an appeals body covering access to public information and a supervisory authority for personal data protection. A total of 30 employees are now employed.

The volume of work dealt with by the Information Commissioner has grown rapidly since the autumn of 2003. In 2006 the Commissioner received 504 complaints and issued 101 decisions related to access to public information issues, 231 reports of violation of personal data protection were received and 180 inspection procedures were carried out. By the year 2010, the number of complaints, related to requests for access to public information had risen to 610 (258 decisions were issued), similarly the number of reports related to the violation of personal data protection also increased, necessitating 712 inspection procedures.

The response from individuals confirms that the Commissioner's work has been effective. As early as 2008 the Politbarometer poll, covering public opinion research on the level of trust people have in public institutions, and with the Information Commissioner included for the first time, showed that 47 % of people polled rated the Commissioner as trustworthy, ranking it fourth behind the President of the Republic of Slovenia (55 %), the Euro (53 %) and the Bank of Slovenia (49 %). The Commissioner was also placed high on the list of the same survey carried out in later years. In January 2013, people surveyed rated the Information Commissioner at the very top of the list of authoritative figures of state supervisory bodies, followed, in equal second place, by the Ombudsman, Zdenka Čebašek - Travnik and the President of the Court of Auditors, Igor Šoltes.

Results of the work of the Information Commissioner are evident also in the general public's high level of awareness. At the end of April 2008, the European Union published the results of the Eurobarometer public opinion survey which looked at the awareness, attitudes and views of citizens of each of the 27 member states with regard to personal data protection as well as their perception of personal data controllers. The poll showed that, as far as understanding the problems, in most of the areas covered in the survey Slovenia ranked at the top of the EU.

In the field of access to public information, protection of the right of access to public information was shown to be at a high level as indicated in the research published in 2013 by the International organisations Access Info Europe (Spain) and Centre for Law and Democracy (Canada), which out of 89 countries, placed Slovenia in an impressive second position with regard to the area of legislative regulation covering access to public information. The increase in the number of complaints in this area, shows that individuals are also becoming more aware of their rights, with which, together with the Commissioner, they are requiring responsible authorities to more effectively implement the Access to Public Information Act.

1.2. Overview of Important Changes for Ensuring Greater Transparency in Slovenia

1.2.1. The most important milestones in the field of transparency:

1. Increased transparency in the use of public funds – Partly as a result of decisions by the Information Commissioner (e.g. Decision No. 020-19/2003/19 of 17 August 2004, wherein a member of the media requested, from the office of the former President of the Republic of Slovenia, a list of names of guests that had attended a dinner hosted by the then President, at Villa Podrožnik), the Access to Public Information Act was amended in 2005 with the provisions of paragraph 3 of Article 6, which provides that information regarding the use of public funds, regardless of possible exemptions, is always to be

publicly available.

2. Increased transparency in public procurement procedures – Also as a result of practices of the Information Commissioner (e.g. Decision No. 021-75/2008/7 and 021-105/2007/9, wherein the applicants, otherwise potential suppliers in particular public tenders, requested access to information of offers submitted in public procurement procedures of various ministries), in 2010 the provisions of Article 22 of the Public Procurement Act were amended to explicitly provide that: quantity specification, price per unit, value of individual items and total value of an offer are public information, and in cases where the most economical offer is sought, other data which influenced the ranking of offers, based on the application of additional criteria.

3. The introduction of the public interest test following amendments to the Access to Public Information Act (ZDIJZ) in 2005 – Prior to the first change to ZDIJZ, the Information Commissioner repeatedly emphasised the importance of balancing the various human rights in procedures regarding requests for access to public information. The public interest test or balance test was for example carried out in 2004, in Case Number 020-10/2004/4, wherein a journalist requested details of the salaries of executive employees at RTV Slovenia.
4. Public sector salary disclosure – Partly as a result of a decision by the Information Commissioner in a matter regarding a journalist's request for details of salaries of former public servants in Case No. 020-10/2004/4, there were changes made to Article 38 of the Public Sector Salary System Act (ZSPJS) in 2005. The provisions of paragraph 6 of Article 38 were added to ZSPJS, which explicitly provides that, in accordance with procedures regulated by the Access to Public Information Act, the individual details of gross wages of every public servant and every public official, before deductions for attachment of earnings, loan repayments or other personal obligations, are to be publicly available.

5. Public disclosure of Notary income – In 2004, in Case No. 020-50/2004, the Information Commissioner dealt with a journalist's request, addressed to a number of Notaries, for information to be forwarded from annual financial statements, of the income and profit derived from carrying out public sector notary work. The Commissioner was of the opinion that such information was freely accessible public information. In proceedings before the Supreme Court of the Republic of Slovenia, the Commissioner's argument was dismissed. However, consequently in 2006, the Notary Act was amended, and in paragraph 2 of Article 2 explicitly provides that the income of notaries, being figures of public trust, be publicly available, thus protecting the reputation of notaryship as a public service and ensuring clients' trust in their work

6. Proactive publication of information of public fund grants – Also as a result of practices of the Information Commissioner, the Eco Fund, for example, began publishing the details of recipients of non-repayable financial incentives, while the ministries published information on recipients of public funds granted through various competitions.

7. Greater transparency in the recruitment of public servants and their contracts of employment – In a number of matters (e.g. Decision No. 021-70/2005/17 of 21 November 2005), the Information Commissioner, using a broad interpretation, which is in the interests of transparency, established good practice for public access to documents relating to the employment contracts of public servants (e.g. documents which indicate if the public servant meets the requirements to fill a given position).

8. Greater transparency of the activities of legal persons governed by public law sui generis – In a number of matters (e.g. Decision against SOD – No. 020-61/2004/21, KAD – No. 090-108/2009, Študentska organizacija Univerze v Mariboru – No. 021-6/2008/1) the Information Commissioner drew attention to the non-transparent activities of legal persons governed by public law sui generis and was of the opinion, that these organisations were also covered by ZDIJZ. On a number of occasions the Supreme Court confirmed that such a view was valid, and the decisions handed down in these cases contributed to more transparent activities of these responsible entities in practice.

9. Establishing good practice in the determination of exempt classified information – In a number of matters (e.g. Decision No. 020-44/2004/3, 021-33/2005/5 and 090-157/2010), the Information Commissioner cautioned, that the assessment as to whether classified

information is exempt needs to be determined extremely restrictively, with reference to material and formal criteria applicable to classified information, as provided for in the Classified Information Act. On the basis of Decision No. 090-157/2010 most of the documents in the so-called trade in arms dealings, between 1991 and 1994, were made publicly available. These documents are largely at the disposal of the Ministry of Defence and the National Assembly of the Republic of Slovenia.

10. The amended Access to Public Information Act, which has extended the circle of responsible authorities to include business entities, which are primarily controlled by the state, local authorities and other legal entities governed by public law – In recent years the Commissioner has repeatedly called on those in authority to move from words to actions, to turn their principle commitments into legal solutions in the interests of transparent operations of business entities owned by the state or local government, and for this reason fully supports the latest changes to ZDIJZ.

11. Adoption of the Council of Europe Convention on Access to Official Documents (Slovenia was among the first 12 signatories) – Slovenia together with Information Commissioner Nataša Pirc Musar, as expert advisor for the Council of Europe, played an important role in the drafting of the Convention, which sets minimum standards with respect to the individual's right of access to official documents. Following successful ratification by the Council of Europe Member States, this right will become internationally recognised as a fundamental human right. Regrettably, Slovenia has not yet ratified the Convention.

1.2.2. Milestone decisions by the Information Commissioner, which have influenced the enforcement of transparency in practice:

In its Decision No. 020-10/2004/4, in a matter concerning the request of a journalist from the Delo newspaper for information on the details of salaries, job performance payments, bonuses and other salary premiums paid to some executive public servants of RTV Slovenia, the Information Commissioner assessed, on the basis of the public interest balance test, together with evaluating the weight of the right to know, as an element of the right to freedom of expression, compared with the weight of the right to protection of personal data, that the requested information was public information – it was in the public interest, and in this particular case the public interest predominated. An appeal was lodged against this particular decision, and with arguments given in court, the Information Commissioner's decision was not upheld. It was this decision however, that paved the way for a wide-ranging public debate on the importance of transparency of salaries in the public sector, as a result of which changes were made to the legislation which regulates the public sector salary system and provides that information relating to public servant salaries is public.

In appeal proceedings no. 021-75/2008/7, the Information Commissioner granted the applicant's appeal in respect of access to the offer documentation of all offerees to the public tender for the supply of cleaning and toiletry materials to the Ministry of Defence, in that part which applies to the adequacy of the product offered by an individual supplier taking into consideration the requirements of the client and the (percentile) level of use of the product offered. The Commissioner determined that in the aforementioned case the information in question was public as it covered a criteria or rather data directly attributable to such criteria, without which it is impossible to determine which offer is the most advantageous or the lowest, which was, for the particular public tender, the primary assessment criteria.

Within the context of the appeal proceedings against the Slovenian Compensation Company (SOD), the Information Commissioner, in Decision No. 020-61/2004/21, determined that the Slovenian Compensation Company was undoubtedly a responsible authority with respect to access to public information. The sole founder and shareholder of SOD is the Republic of Slovenia, having also contributed the legally required share capital, while the Government of the Republic of Slovenia has competences of the authority's General Assembly.

In Decision No. 021-33/2005/5, within the context of appeal proceedings in which the applicant addressed a request to the Ministry of Finance for access to an analysis of the state of the gambling market in Slovenia, the Information Commissioner determined that this was also freely accessible public information. The requested document, although marked as confidential, did not in its content display any of the characteristics of a confidential document

as set out in the provisions of paragraph 5 of the Classified Information Act.

Based on a request from two journalists made to the National Assembly of the Republic of Slovenia for access to all documents relating to the trade in arms between 1990 and 1994, which were the result of work carried out by the Commissions for Parliamentary Inquiries in numerous appeal proceedings (namely in appeal proceedings no. 090-157/2010, 090-101/2010 and 090-32/2009), the Information Commissioner examined a few thousand documents and in the course of two years issued 11 decisions, which allowed the applicants access to some thousand documents connected with the infamous arms affair. During the appeal procedure special attention was required, not only because of the magnitude of the information requested, but also because of the extremely large volume of personal data contained therein, and the process of establishing the legality of individual so identified confidential documents.

In appeal proceedings no. 090-161/2009, the Information Commissioner dealt with an applicant's appeal against a decision from the Ministry of Health in which the applicant's request to view the contract between the Ministry and a pharmaceutical company which was supplying a vaccine against a new influenza virus, was denied. The Information Commissioner concluded that public interest in the disclosure of information that related to the risk, guarantee, responsibility for the vaccine as well as compensation and limitations of responsibility, outweighed the private interest of the company to protect such information as a trade secret. The Information Commissioner assessed that the contract did not represent a trade secret in its entirety, because in part, the information with regard to the use of public funds was already public as required by legislation, and in part it was concluded, that the public interest in being informed prevailed and that it was necessary to disclose the requested information pursuant to paragraph 2 of Article 6 of ZDIJZ.

In 2007, in connection with an applicant's request for information on the allocation of humanitarian aid funds following floods, the Information Commissioner handed down a decision (Decision no. 0900-23/2008/13), that freely available public information in this case included details of donations received following the floods, individually referenced but without the names of recipients, together with details listing the names of legal persons and individuals who were recipients of humanitarian aid following the floods, as this information was related to the use of public funds, which notwithstanding that this information is of a personal nature, represents freely accessible public information.

In an appeal regarding a request for the most recent available version of topographic layers for the whole of Slovenia to be forwarded electronically, for the purposes of non-profitable re-use, the Information Commissioner decided (Decision No. 021-54/2006/3), that this was freely available public information which the authority must forward to the applicant free of charge. The Commissioner stressed that it is crucial for the re-use of information, that public sector authorities gather information primarily for the purpose of carrying out their public duties, and that information already gathered, if it is classified as freely available public information, must be available to applicants and forwarded for further use for both profit or non-profit purposes. Information gathered by the public sector is financed by public budgetary funds and as such is the property of those who contribute to budgetary funds, namely all citizens; such information is not therefore the property of the authority where it was generated. The fact that the authority itself can be a re-user of the information which is generated during the carrying out of its public functions, does not change the provisions of the law which require that the authority must apply the principles of non-discrimination and enable the re-use of such information, under the same conditions, to all interested applicants. Pursuant to Article 34(a) of ZDIJZ an authority can charge a fee for the re-use of information if it is to be used for profit making purposes. Considering the fact, that from the applicant's request it was obvious that the requested information was to be used for non-profit purposes, the aforementioned provisions did not apply.

In the matter concerning a journalist's request for the forwarding of a transcription of a session of the Government of the Republic of Slovenia in which it adopted a resolution regarding the gratuitous transfer of its share in Splošna plovba, d. o. o., to the Slovenian Compensation Corporation, (Decision No. 090-178/2010/6) and further to an appeal being lodged, the Information Commissioner considered that the information was freely accessible public information. The Government was unable to argue an exemption for internal functioning, that is it was unable to demonstrate how the forwarding of the requested document to the

applicant would cause serious disturbance to the government's future work.

In appeal proceedings concerning the forwarding of a contract for a public-private partnership between the Municipality of Maribor and Iskra sistemi, d. d., for the project "Upgrade and automatisation of road traffic in the Municipality of Maribor" covering the installation of traffic radar (Decision No. 090-190/2012/14), the Information Commissioner's decision was that part of the requested documents represented freely accessible public information. Although the authority had not directly paid the private partner any moneys from the municipality's budget, it is apparent that the subject of the concluded contract would undoubtedly be financed from public funds, that is those funds derived from recovered traffic fines. In addition, information which indicates if the authority followed the recommended guidelines of public-private partnerships, and if it selected an appropriate offer and consequently entered into a contract, which was in accordance with the provisions of the regulations covering such contracts, cannot be considered a trade secret. Similarly, parts of the offer or the contract cannot be protected as trade secrets, in as much as the information relates to specification of quantities, price per unit, value of individual items and total value of the offer, or other details which confirm the fulfilment of set requirements, including information that affected the ranking of offers based on other specified criteria, as this information is already, by law, public. As for those parts of the contract, which concern the responsibilities of the private partner, the responsibilities of the public partner, the maintenance and administration of the system and the operation of the minor offences system, which were correctly identified as trade secrets, the Information Commissioner assessed that it was necessary to disclose them pursuant to paragraph 2 of Article 6 of ZDIJZ, and based on the predominance of the public interest. The assessment was that the public interest in disclosing the information was greater than the damage that could arise from the disclosed information. Questions regarding what kind of responsibilities the council had taken upon itself in terms of the public-private partnership and what responsibilities it had transferred to the private law entity (the third-party participant), in important areas such as regulation of and safety in road traffic, can indeed never be outside the realm of the public interest. For the remainder of the contract the Information Commissioner took the position that there was not a predominant public interest and that access to information which represents trade secrets must be denied.

1.3. Overview of Important Changes for Ensuring Personal Data Protection in Slovenia

1.3.1. The most important milestones in the field of personal data protection:

1. Limiting the excessive publication of personal data of individuals through the Real Estate Register – As a result of a request for a constitutional review, which the Information Commissioner (re)submitted in 2011, the Constitutional Court repealed the provisions of the first and the second paragraphs of Article 114 of the Real-Estate Recording Act, which provided that data recorded in the land register and building register, namely in that part which applied to data relating to the owner, if they were a natural person, was public. Thus the Constitutional Court clearly expressed its view that the publication of personal data for a specific purpose (for instance in the land register) does not mean that these data are absolutely public nor that their further processing for any purpose is allowed. With this aforementioned provision land surveyors circumvented the decision of the Constitutional Court from 2007, wherein Constitutional Court judges had, at the request of the Information Commissioner, repealed part of the same law, which provided that the Real Estate Register should be public with regard to the data on natural persons.

2. Ensuring the lawfulness of invasions of privacy and personal data protection conducted by the Slovene Intelligence and Security Agency – In 2008, the Information Commissioner filed a request for a constitutional review of the Slovene Intelligence and Security Agency Act (ZSOVA) and alerted to the provisions of Article 21 of ZSOVA, on the basis of which a database of personal data was being created in connection with the strategic monitoring of telecommunications and which was, in the Commissioner's opinion, unconstitutional. The Constitutional Court dismissed the request on procedural grounds and made no decision on its merits. For this reason we are still without a decisive position from our highest court

on an important point of law regarding the acceptability of the behaviour of the Slovene Intelligence and Security Agency in terms of invasion of the constitutionally protected right of communication privacy of the individual.

3. Limiting the invasion of (electronic) communication privacy of individuals by supervisory authorities – With a request for a constitutional review of the provisions of Article 29 of the Prevention of Restriction of Competition Act (ZPOmK-1) the Information Commissioner drew attention to the question of the acceptability of the behaviour of supervisory authorities, which exercise their competences within a framework of administrative and inspection procedures and/or minor offence proceedings and on the basis of legal provisions, but without a court order and outside the purposes as stipulated in Article 37 of the Constitution of the Republic of Slovenia, make invasions into (electronic) communication. The Constitutional Court had adopted a position on the content of communication privacy in the past; however, it had never expressed its position on the competences of supervisory and administrative authorities. Within the scope of an inspection procedure against the Competition Protection Office of the Republic of Slovenia (now the Slovenian Competition Protection Agency), instigated because it was examining and recording the e-mails of employees of the company Produkcija Plus d.o.o.(No. 0612-166/2011), the Information Commissioner assessed that the Competition Protection Office of the Republic of Slovenia had examined e-mails in a manner which was not compatible with constitutionally protected communication privacy and therefore filed a request for a constitutional review of the provisions of the Article 29 of ZPOmK-1. As a result of the Constitutional Court's dismissal of the request on procedural grounds, we remain without an urgently needed position of the highest court on the question of the acceptability of the invasion of the constitutionally protected right to communication privacy by supervisory authorities.

4. Ensuring the proportionality of the invasion of privacy of individuals in a tax procedure – the publication of tax non-payers – With a request for a constitutional review of provisions in the law, the Information Commissioner alerted to the possible unconstitutional nature of some provisions of Article 20 of the Tax Procedure Act (ZDavP-2), which refer to the measure taken in the form of the publication of tax non-payers. In the opinion of the Commissioner, the measure is not necessary nor appropriate for achieving the objective, for which it was adopted, and, at the same time, is not in proportion to (non-existent) positive effects, which it is supposed to bring. The list of non-payers includes individuals with very diverse life stories and by treating them all equally, and thus disproportionately, unfairly exposes them on the same 'shameful list', while the essence of the problem remains hidden from the public – what has the state done to collect taxes due? The Constitutional Court has yet to hand down a decision in the matter.

5. The unacceptability of the excessive legal measure requiring obligatory retention of electronic communication traffic data – With the filing of a request for the constitutional review of some of the provisions of paragraph thirteen of the Electronic Communications Act (ZEKom-1) regarding the obligatory retention of data on traffic and location and other related data, which identify the subscriber or the user of public communication services, the Information Commissioner alerted to the fact that these measures are not in accordance with the proportionality principle and the contents of Directive 2006/24/EC of 15 March 2006. The Constitutional Courts of Germany, Romania, the Czech Republic and the High Court of Ireland have already recognised this measure of obligatory retention of electronic communication traffic data as objectionable, arguing that it violates certain rights and freedoms of individuals. On the initiative of Austria and Ireland for an assessment as to whether the Directive was in conformity with the Convention for the Protection of Human Rights and Fundamental Freedoms, the Court of Justice of the European Communities repealed the Directive. The Constitutional Court of the Republic of Slovenia has yet to make a decision on the request.

6. Establishing good practice with regard to the collection of personal data for the purposes of fulfilling a contract – With the decision in inspection procedure (No. 0613-144/2011) regarding the„BicikeLJ city bicycle hire service vs. Europlakat d.o.o., the Information Commissioner alerted to the allowable limits of personal data processing for the purposes of entering into and fulfilling contracts between responsible entities and users. The Information Commissioner ordered the responsible entity in this case to cease collecting personal data (inter alia data on gender and mobile phone numbers), for which it had no appropriate legal grounds (the contract could namely be concluded and fulfilled without these data, also the responsible entity did not obtain users' consent for the processing of such data). In its

decision, the Information Commissioner clearly distinguished between personal data, which are necessary (e.g. first and last name, address, date of birth, e-mail address, PIN number, bank account number and the bank identification code, credit card information), and data, which are not necessary for the fulfilment of the contract. The Information Commissioner also pointed out that this was a public-private partnership between the responsible entity, the company Europlakat d.o.o., and the Municipality of Ljubljana, which is why, in this instance the responsible entity does not enjoy the contractual freedom to independently decide which personal data it will require from users of the service. The Constitutional Court of the Republic of Slovenia confirmed the decision of the Commissioner, dismissing the action instigated by the responsible entity in the administrative dispute.

7. Establishing appropriate practice with regard to the invasion of personal privacy and the data of employees' telephone conversations – In two high-profile inspection procedures, namely a procedure at the Ljubljana District Court (Case No. 0603-154/2009) and the Ministry of Foreign Affairs (Case No. 0612-19/2008), the Information Commissioner alerted to the unresolved problem of insufficient legal regulation in the area of workplace privacy in the Republic of Slovenia, and with its own practices contributed to improvements in this area. In both cases, the court confirmed the Commissioner's decision. Moreover, the Commissioner has on a number of occasions, called for legislation to be adopted, which would clearly regulate this area, and even sent a draft proposal for a Workplace Privacy Act to the competent ministry.

8. Establishing appropriate practice with regard to the protection of medical records – With several inspection procedures the Information Commissioner alerted to the importance and urgency of appropriate protection of sensitive personal data in larger hospitals and health care centres. In all cases, the Commissioner ordered the establishment of appropriate measures for ensuring physical and technical personal data protection, including the introduction of daily logs enabling the traceability of personal data processing and the necessity of concluding a written contract for the contractual processing of personal data and ensuring additional controls, when health care providers give authorisation for specific tasks relating to the processing of personal data (e.g. for transport, destruction of medical files, etc.), to external contractors.

9. Ensuring lawful processing of personal data by those initiating a call for a municipal referendum – In the inspection procedure against the Municipality of Borovnica and lawyer Andrej Doles (Nos. 0612-54/2008 and 0603-36/2008), the Information Commissioner determined that the Mayor and lawyer Andrej Doles unlawfully processed personal data. The Mayor namely forwarded the initiative from voters calling for a referendum with regard to the building of residential dwellings in the municipality, together with a list of 420 signatories with their personal data, to the lawyer representing the company Orbital d.o.o., which later that same day mailed all signatories insisting that they immediately cancel their signature, threatening them with the intention to file a civil claim for damages if they failed to do so. Neither the Mayor nor the lawyer had adequate legal grounds for the described processing of personal data of signatories to the initiative; therefore, in accordance with recourse available for such violations in minor offence proceedings, each of them was fined by the Commissioner. The Attorneys Act does not grant any general powers to lawyers for the collection and use of all personal data. The Court confirmed the decision of the Commissioner and dismissed a request for judicial protection.

10. Prohibiting the illegal monitoring of employees' e-mails – Within the scope of an inspection procedure at the Slovenian Research Agency (No. 0612-81/2008) the Information Commissioner discovered the illegal examination and subsequent processing of traffic data on e-mails received by employees on the Agency's mail servers for the supposed purpose of reducing the burden on the mail server (by limiting private e-mails which include larger attachments). The Commissioner ordered the Agency to amend their rules which allowed such policy and to stop monitoring e-mails on its mail servers. The decision of the Commissioner was also confirmed by the court.

1.3.2. Milestone decisions by the Information Commissioner, which have influenced the provision of personal data protection in practice:

In the case of violations at the Ljubljana District Court (Case No. 0603-154/2009) the

Information Commissioner discovered the illegal collection and use of data on the calls made by a judge from their work mobile phone (date and time of the call, the called telephone number or the number of the SMS/MMS recipient, call duration, the amount and the type of the provided service). The responsible authority had collected the data in order to document communication with regard to a bomb explosion at the home of Judge Katarina Turk Lukan, and to determine, which person at the Court, using a work mobile phone, had communicated with journalists. Illegal use of telephone conversation records in a fixed telecommunications network (a list of around 110,000 incoming and outgoing calls) was also discovered at the Ministry of Foreign Affairs (Case No. 0612-19/2008). The records were being used for internal control purposes at the Ministry, in order to identify a person who had supposedly forwarded a document from the Embassy of the Republic of Slovenia in Washington to a journalist. In order to implement further measures of internal control, the commission investigating the matter reviewed the list of calls and looked for users who had contacted a certain newspaper publisher by telephone. Not only was the list illegally obtained, also illegal was the data mining of the illegally obtained database with the help of a search engine. Data on the called and the calling telephone numbers are protected in accordance with Articles 38 and 37 of the Constitution of the Republic of Slovenia. In both cases, the court confirmed the Commissioner's decisions.

In another inspection procedure the Information Commissioner dealt with a case of the inadequate protection of sensitive personal data (Case Nos. 0612-1/2008 and 0603-4/2008). During their transport for destruction, i.e. thermal destruction, an unidentified number of cardboard boxes filled with internal order forms for laboratory examinations from the Celje Healthcare Centre, fell out of the truck transporting them. Further, during an examination of the facilities of the Institute of Oncology Ljubljana (Case No. 0612-48/2008) the Information Commissioner discovered that medical files (the medical records of deceased patients) were stored in more than a hundred open cardboard boxes in a hallway, which was unlocked at the time of construction or during the working hours of construction workers. The Information Commissioner also carried out ex officio preventive inspection initiatives (several cases, e.g. No. 0612-81/2007) in all larger hospitals and healthcare centres in order to verify procedures and measures for personal data protection.

Within the framework of an inspection at the Office of the Republic of Slovenia for Gaming Supervision (No. 0612-11/2012), the Information Commissioner warned that it was unacceptable to enable public access to web statistics on data relating to web page visits of the responsible authority in question (data on date and time of the visit, visitor's IP-address, search environment, referral and other web page data). By enabling such access the responsible authority did not adequately protect the above mentioned personal data. Moreover, the Commissioner pointed out that without applicable legal grounds (by law or personal consent of the individual) the automatic redirection of web page visitors (to www.infounpis.si) to other web addresses and the subsequent establishment of a database of personal data on individuals, who wished to visit other web pages, was unacceptable. In this specific case, the redirection enabled the responsible authority to collect personal data of individuals, who did not wish to visit its web page, but web pages with on-line casinos, which offer on-line gambling without government concession (e.g. web pages of blocked on-line betting sites). Following the Commissioner's decision, the responsible authority disabled the public accessibility of data, configured the server to prevent the recording of IP addresses and erased data from the log files, which represented personal data of individuals, who were redirected from other web pages to the web page of the responsible authority in question. At the same time, the responsible authority filed an action against the Commissioner's decision in the Administrative Court of the Republic of Slovenia, because it did not agree that data, which the Information Commissioner ordered to be erased and no longer recorded, were personal data. The Court has yet to make a decision in this administrative dispute.

At the end of 2011, the Novo mesto District Court confirmed the largest fine ever imposed by the Information Commissioner, on an insurance company for the illegal processing of personal data (Case Nos. 0613-178/2009, 0603-111/2009 and 0603-112/2009). In the minor offence proceedings the Information Commissioner established that an insurance company forwarded personal data of 2,382 former policy holders to a second insurance company without any legal grounds or personal consent from the individuals, to whom the data referred. The second insurance company used the data for direct marketing purposes. The Court dismissed the request for judicial protection, filed by the offenders, and confirmed the decision which included a fine in the amount of 112,590 EUR, imposed upon the legal entity,

and a fine in the amount of 20,000 EUR imposed upon the responsible person.

During an inspection procedure at the Tax Administration of the Republic of Slovenia (DURS) (No. 0612-91/2008) in order to verify the legality of access to the tax register by DURS employees, the Information Commissioner alerted to the obligations of all users to ensure compliance with the provisions of the Personal Data Protection Act in practice. On the basis of the traceability principle, the Information Commissioner scrutinised how public servants complied with personal data protection in various public administration registers, namely if there existed justification for access to the register of taxpayers. The Commissioner sought an explanation of the reasons for access from every employee. During the procedure it was established that 47 of the 200 employees scrutinised accessed documentation on the basis of the only legally permitted reason, namely in order to conduct a tax procedure. The remaining 153 employees had no justifiable reason for access to the information. The most common reason given was curiosity. Due to the processing of personal data without applicable legal grounds and the resulting violation of Article 8 of ZVOP-1, the Information Commissioner issued a warning to the offenders, as a lesson to other public servants, that they cannot 'browse' through personal data without justified reason.

In 2007, through a contractual agreement with processing company KRO, d.o.o., the Tax Administration of the Republic of Slovenia sent tax declarations, filled out in advance, in an inappropriate manner (Case No. 0612-52/2007), which resulted in minor offence proceedings wherein the Information Commissioner established that there had been a violation of the rules regarding personal data protection by both responsible entities. Tax declarations were not sealed properly, because they were only spot-sealed instead of being sealed along the entire length of the envelope, and it was therefore possible to view confidential tax data, while some recipients even received tax declarations, filled out in advance, that had been opened. The responsible authority immediately rectified the mistake and stopped sending tax declarations, filled out in advance. All later tax declarations were sent inserted in a plastic foil, which was closed, and additionally thoroughly sealed and glued. Documentation with personal data of taxable persons, because of sensitivity (tax secrecy), if sent by regular mail, must be sealed in these envelopes, so the contents can only be accessed by visibly damaging the envelope. Further the sealed envelope must be protected with protective print, so that the content of the envelope or personal data included in the tax declaration is not visible under daylight or if it is exposed to normal lamp light.

In the Information Commissioner's decision (Case No. 0613-4/2006), confirmed also by the Ljubljana District Court, it was concluded, that the publication of the first and last names of employees who receive the highest gross and net wages at the weekly newspaper publisher Demokracija was illegal. The weekly newspaper publisher had no legal grounds for the publication of personal data of 86 employees neither did it have the personal consent of individuals and the level of wages paid is public data only for the public sector. The publisher referred to the right to the freedom of speech which is already limited by the Media Act, pursuant to which the weekly paper could justifiably obtain and publish controversial data only if it were to prevent serious crime or imminent danger to people's lives and their property; which in the current case could not be said. The publication of data infringed upon the constitutional right to personal dignity, protection of privacy and personality rights, and the right to personal data protection. The right to the freedom of speech did not prevail in this »collision« of rights.

In 2009, the Information Commissioner performed systematic controls covering personal data protection in the banking sector (Case No. 0613-336/2009) in order to verify the legality of the processing of personal data during the interbank data exchange of the credit standing of their customers within the framework of the newly established system SISBON, and also the legality of the accessing of data in customer accounts. It was concluded that there was no illegal access to data during the interbank data exchange. However, during verification of access to data of some well-known Slovenian individuals, which was carried out at the six largest Slovenian banks, it was discovered that in two banks illegal access to data had occurred. The Information Commissioner imposed sanctions against bank employees who had illegally accessed data in customers' personal accounts.

On the basis of a complaint, the Information Commissioner discovered that the personal data of dog owners were illegally obtained by some veterinary clinics for the purpose of direct marketing (several cases, e.g. No. 0603-38/2011). On the basis of traceability logs for the

processing of dog owners' personal data in the central dog registry (which is managed by the Veterinary Administration of the Republic of Slovenia) the Commissioner concluded that using personal data from the registry, veterinary clinics send notifications to dog owners regarding rabies vaccination for their dog, in which they are sent general information and the time frame in which vaccination will be carried out, frequently dog owners are also offered other services (e.g. vaccinations against contagious diseases, sterilisation and castration). Such use of data from the registry, which is not a public registry, is unauthorised. Said data are not available to the public and can therefore be processed only for purposes, allowed by law, which does not include their use for direct marketing. For direct marketing, veterinary clinics can only use personal data of dog owners, who are their clients, or that personal data, which they obtain within the lawful pursuit of their business activities, and data, which they obtain from publicly accessible sources.

The Information Commissioner ordered the National Electoral Commission to erase personal data of candidates for the National Assembly elections held in 2008, 2004 and 2000, and local elections held in 2010, 2006 and 1998 (name, date of birth, place of birth, address, qualifications and current job) from the Commission's web pages (Case No. 0612-192/2011). The sector-specific National Assembly Elections Act, which specifies how the lists of approved candidates in the electoral unit and lists of candidates, who are voted for in individual electoral districts, should be drafted and published, only allows for such processing of a candidate's personal data prior to the elections and does not regulate their publication after the elections. The purpose of the processing of personal data, namely their publication on the web pages, had been accomplished and the election results could not be challenged with any further legal remedies, therefore the Information Commissioner decided that the responsible authority had no legal grounds for their (further) processing.

The Information Commissioner prohibited Ljubljana potniški promet, d.o.o. (LPP, d.o.o.) from collecting data on the location of holders of the Urbana non-transferable pre-paid travel cards, because during the inspection procedure (Case No. 0613-246/2009) it was determined that the company randomly collected and retained data on time, place and bus line (data on location) of all passengers, who paid for transport with the Urbana non-transferable pre-paid travel card, even though it had no legal grounds for the processing of this data. On the basis of the decision of the Commissioner, LPP, d.o.o. had to stop collecting data on the location of passengers who paid for transport with non-transferable pre-paid cards and erase the above mentioned data from all their personal data databases. During the inspection procedure the Commissioner determined that personal data was processed only if the green Urbana card was used, which is issued to a specific holder and is non-transferable. On the other hand, travellers can use the yellow Urbana card anonymously with none of their personal data being processed.

During another inspection procedure (No. 0613-263/2010) the Information Commissioner concluded that the publication of the bill of indictment in the Patria case on the Janez Janša Facebook profile was an illegal processing of personal data of persons, against whom the above mentioned bill of indictment had been filed. For this reason, the Information Commissioner ordered the person responsible, who manages the on-line profile, to remove the above mentioned bill of indictment from the web page. In the case concerned, the Information Commissioner also filed a criminal complaint, which was dismissed by the Ljubljana District State Prosecutor`s Office, since the minor importance of the criminal offence compared with the consequences that would arise from criminal prosecution proceedings, was disproportionate.

In the inspection procedure against the Municipality of Ljubljana and the Zoran Janković Political Party – Positive Slovenia, the Information Commissioner suspected that personal data of pupils from the Koseze Elementary School, who were photographed with the Mayor of Ljubljana, Zoran Janković, were illegally processed, because their photograph was later published in the Positive Slovenia newspaper Bolje in November 2011 (for purposes of the election campaign for the early National Assembly elections in 2011), and established that personal data of pupils taken from the photograph album of the Municipality of Ljubljana, were illegally forwarded and used for the Positive Slovenia election campaign. In its newspaper, Positive Slovenia published a photograph, shot by an official (contracted) photographer of the Municipality of Ljubljana in order to document the Mayor's visit to the elementary school. The Commissioner imposed a fine on Positive Slovenia, its responsible person and sanctioned the photographer, who had illegally forwarded the photograph to the agency in charge of the

newspaper.

Following an inspection procedure the Information Commissioner concluded that some parts of the provisions of Article 128 of the Aviation Act, which regulates movement and remaining at the public airport and within the facilities of the air traffic navigation services, were unconstitutional. This is why, in 2006, the Commissioner filed a request for a constitutional review. In the opinion of the Commissioner, the challenged Article severely invaded information privacy as an individual's constitutional right, with an excessive collection of personal data planned, which is not proportional to the benefit to the community and general national safety, which would be essential in a democratic society. Moreover, the challenged provision of the Act provides only a non-exhaustive list of personal data which are supposed to be collected, and does not specify the data, as is required by the Constitution of the Republic of Slovenia. The Constitutional Court for the most part acceded to the request of the Information Commissioner.

The Information Commissioner filed a request for a constitutional review of Article 45 of the Ordinance on Road Traffic Regulation of the Municipality of Ljubljana, which specifies that the municipality can install video-surveillance systems on public roads and in other public areas in the municipality to monitor traffic conditions and compliance with traffic regulations, to improve traffic fluidity and traffic safety and with this collect personal data. The Information Commissioner raised a key question, namely whether the processing of personal data of individuals can be considered as a fundamental function of the local community, that is as a function or competence, wherein the local community can make totally independent decisions, with ordinances establish new personal data databases, decide on their content, etc. In the opinion of the Information Commissioner, this is not the case. The conduct of all local communities in the future on one hand, and the level of personal data protection in the Republic of Slovenia on the other hand, depend on the answer to this question. The Constitutional Court has yet to make a decision on this matter.

1.4. Other Important areas of Work of the Information Commissioner in the past ten years

Throughout these years, the Information Commissioner has paid a lot of attention to increasing awareness regarding privacy and personal data protection. The Commissioner has designed a broad spectrum of activities, endeavouring to make them both preventive and educational.

One of the most important activities in this area is the issuing of non-binding opinions on many questions of personal data protection. Most of the opinions are available on the Information Commissioner's web page and represent a comprehensive knowledge base, which is a great help to personal data controllers. We feel that we can confidently claim that such a large number of published opinions cannot be found at any other supervisory authority for personal data protection in the EU.

In addition to opinions, the Commissioner also prepares guidelines, providing answers to the most frequently asked questions in certain thematic areas. In several cases, the Information Commissioner was among the first in the EU, to issue guidelines for certain areas (e.g. cloud computing, digital television, intelligent video-analysis). Together with guidelines the Commissioner also prepared reports, for instance the Report on Personal Data Protection in Loyalty Programmes.

The Information Commissioner maintains a strong presence on the internet, which it uses for efficient communication with its target public. The Information Commissioner invested heavily in its web image and received a Netko award for the best web page in the public administration category in 2008. It also has a profile on the Facebook social network and is one of the most interesting and influential Twitter users.

The Information Commissioner also introduced awards for good practice to encourage good solutions in the area of personal data protection. Every year it presents a special award to representatives from the public and private sectors, who have demonstrated consistent compliance with the law or instigated successful measures for personal data protection.

In 2008, the award was presented for the first time, its recipient being the Health Insurance Institute of Slovenia for its efforts to ensure suitable information solutions in the area of personal data database protection during the introduction of some systems for the processing of personal data, and to the Livar company from Ivančna Gorica for the exemplary regulation of personal data protection, which was demonstrated during an unannounced inspection. Other award-winners were: in 2009: Cetis d.d. for an exceptionally detailed and effective system of organisational, technical, and logical-technical procedures and measures for personal data protection and the Ministry of Defence of the Republic of Slovenia for an exceptionally accurately designed system of competences for the processing of personal data, implemented with military diligence; in 2010: the Dr. Janko Benedik Care Home from Radovljica for a detailed and effective system of procedures and measures for personal data protection in relation to video-surveillance operation and Iskraemeco, merjenje in upravljanje energije, d.d., an energy measurement and management company, for a detailed system of competences for the processing of personal data; in 2011: Društvo življenje brez nasilja (the Life Without Violence Society), which ensured excellent protection of their clients' sensitive personal data and the public institution Obalna lekarna Koper, for excellent protection of its customers' medical data; in 2012 the Commissioner did not present the award and in 2013 it was presented to the Supreme Court of the Republic of Slovenia for the electronic land register and Zavarovalnica Maribor, an insurance company, for appropriate personal data protection, determined during an inspection.

Since 2008 the Information Commissioner has also presented awards for attainment of the ISO/IEC 27001:2005 certificate for information security management systems so promoting the use of this international standard, which allows for comprehensive information security management, which is an important part of personal data protection. In 2011, the Information Commissioner first presented the award of Privacy Ambassador, which is a special award for efforts in the area of so called privacy by design, which emphasises proactive personal data protection and shows that legitimate goals can often be achieved with minimal or in fact no invasion of privacy. In 2011 the first Privacy Ambassador became the Metrology Institute of the Republic of Slovenia, for its efforts in the area of personal data protection with regard to the so called sectoral traffic speed measuring. In 2012 the Privacy Ambassadors were: Stanka Šalamun, Renata Stupar, the Acros company team for its work on the SLED project, in the framework of which they reminded several personal data controllers of the right of every individual to be notified of their own personal data and pointed out the importance of proactive operation in the spirit of the privacy by design principle. In 2013 the Privacy Ambassador became the IT and E-Services Directorate, the Ministry of Public Administration and Justice and employees mag. Aleš Pelan and dr. Alenka Žužek Nemec for ensuring privacy by design in their successful work on the European STORK, SPOCS and STORK 2.0 projects and other projects, and for their preparation of an Analysis of possibilities for introducing more secure and user-friendly e-identities.

The Information Commissioner also devoted a lot of attention to ex-ante privacy impact assessments. The Information Commissioner experts provided answers to many issues that were encountered by numerous public and private sector organisations during the introduction of new systems, legislative solutions, changes to business processes and interpretation of legislative requirements. We are confident that with this type of preventive action we have prevented many violations and helped in the design of better solutions.

The Information Commissioner was actively involved in many groups, among others an inter ministerial task force, in cooperation with the Ministry of Public Administration, the Ministry of the Interior and the Ministry of Higher Education, Science and Technology. which concerned itself with the introduction of more secure and user-friendly e-identities, carrying out a comprehensive analysis of e-identity status in Slovenia, an analysis of possible legal and implementation possibilities, and a comparative analysis with other countries. Surveys and consultations with participants, such as service providers, certification authorities, citizens and public servants, were conducted. The e-identity system improvements enable better and more efficient e-government services, which are more frequently used by target groups, while at the same time, such improvements accompanied by appropriate decisions, enable a higher level of personal data protection than is offered by current means of identification and authentication of individuals in a virtual environment.

Since its establishment, the Information Commissioner has paid a great deal of attention to monitoring shifts and changes in the legislation in the area of access to public information

and especially in the area of personal data protection, in which sector-specific rules define individual personal data databases, processing and storage methods and other aspects of invasion of privacy of individuals in relation to the processing of personal data. The Information Commissioner is often critical of the ease, recklessness and inconsistency, with which those proposing legislation often try to introduce various new forms and methods of personal data collection, without weighing the necessity of invasions of privacy in relation to their benefits, without careful thought and consideration of the consequences of individual legislative solutions, when they try to link existing large personal data databases or introduce new personal data databases without showing any sensitivity for the consequences of these legislative solutions and above all without consideration for possible abuses. Among other things, by issuing warnings the Information Commissioner also became actively involved in the procedure of amending the Electronic Communications Act, Police Tasks and Powers Act and Criminal Procedure Act. Annually, the Commissioner gives opinions on about 50 regulatory proposals (more than 100 in 2013) and the degree to which these are taken into account by regulatory authorities varies greatly. It often happens that some do not heed warnings related to personal data protection or they underestimate the importance of the individual's privacy. As a consequence, regulations are introduced which disproportionately invade individuals' privacy, bringing no benefits for the government or society which would justify the reckless and invasive legislative solutions that are adopted. On the basis of the Commissioner's initiative for the constitutional review of the provisions of Article 62 and 62d. of the Health Care and Health Insurance Act, the provisions of Article 390 of the Banking Act and the provisions of Articles 47, 58, 123, 165, 247, 334, 432 and 543 of the Financial Instruments Market Act, which in the opinion of the Commissioner were unconstitutional, appropriate changes were made to the law which resolved the question of constitutionality.

A good example of the interactive role of the Information Commissioner is the regulation of competences for locating mobile phones, when life and limb of the individual is endangered (Article 104a. or new Article 153 of the Electronic Communications Act). At the initiative of and with cooperation from the Commissioner, a carefully prepared legal framework arose together with procedures which were defined in detail, which in practice enabled a transition from legal uncertainty and time-consuming procedures to an effective exercise of powers and consequently the successful rescue of human lives. Due to this special involvement of Information Commissioner experts the reformed procedures will be faster, data will be more useful and the control will be enhanced. This is a good example of how an otherwise very invasive authorisation can be regulated in detail and regularly controlled, making it therefore proportional and effective.

The Information Commissioner, as one of the first and still rare public authorities, had its internal regulations, which are prerequisite formal conditions for a transition to an e-storage system for documents and archives, approved by the Archives of the Republic of Slovenia in 2011.

1.5. The influence of the Commissioner on developments in the fields of Transparency and Personal Data Protection both Internationally and within the European Union, and collaboration in International projects

Since its establishment, the Information Commissioner has gained a considerable reputation as well as trust among colleagues from other European Union Member States. The International Working Group on Data Protection in Telecommunications (IWGDPT or the Berlin Group) thus adopted the Sofia Memorandum, which is based on the work of the Information Commissioner and represents a milestone with regard to issues related to personal data protection in the area of satellite-based road tolling. Within the framework of international activities, the Commissioner, by offering opinions, is actively involved in the preparation of a new regulation on personal data protection in the EU.

In 2013 the Information Commissioner Nataša Pirc Musar was appointed by the European Commission to a special ad-hoc EU-USA group, which sought to determine the actual state of activities of the National Security Agency (NSA) in relation to the mass collection of information

and personal data of European Union citizens and at its conclusion prepared a special report.

The work of the Information Commissioner was also very highly regarded in the accession process of Slovenia to the OECD.

In addition to its participation in the meetings and working sub-groups of the Article 29 Data Protection Working Party and in the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108), the Information Commissioner has, since its inception, also been actively cooperating in European personal data »mega-databases« surveillance bodies, such as: the Schengen Information System, Europol, Visa Information System and Eurodac. Among other activities, the Information Commissioner also participated in the joint monitoring operation in relation to the implementation of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Since 2012, the Slovenian Information Commissioner, Nataša Pirc Musar, has been the Chair of the Joint Supervisory Body of Europol (prior to this she was the Deputy Chair). In addition, the Commissioner played an important role in Slovenia's entry into the Schengen Area in terms of ensuring an adequate level of personal data protection. Together with its employees, the Commissioner was also involved in compliance assessment of the level of personal data protection in other countries (e.g. Switzerland, Romania and Bulgaria).

In 2012, the Slovenian Information Commissioner together with the Serbian Information Commissioner also successfully carried out the International Twinning Light Project, which focused on the improvement of personal data protection in Serbia and the enhancement of the national supervisory authority for personal data protection. Information Commissioner experts were successfully involved in a similar project in Montenegro and the European LAPSI project (Legal Aspects of Public Sector Information). Its purpose was to establish a thematic network of experts in the area of public information re-use.

In cooperation with the line ministry, the Information Commissioner successfully presented a model for cross-border e-government services, which allows an individual to maintain control over their personal data. The so called STORK approach, which is based on the right of an individual to access their own personal data, also convinced other EU Member States, which are trying to establish cross-boarder e-government services.

Representatives of the Information Commissioner annually attended and presented contributions at many international conferences and events (e.g. at the European and Global Conference of Information Commissioners). As part of the activities for raising public awareness, the Commissioner celebrates annually, on 28 January, European Data Protection Day, and on 28 September, International Right to Know Day.

1.6. The Information Commissioner's assessment of key challenges in the field of Transparency over the next five years

1. One of the key challenges in the field of public information access is above all the implementation of the latest amendments to the Public Information Access Act (ZDIJZ) in practice, which has extended the circle of responsible authorities to business entities, which are primarily controlled by the state, local communities and other legal entities, governed by public law.

2. Another key challenge is also the issue of the transposition of the amendments to the directive on the re-use of public sector information into Slovenian legislation and its effective implementation in practice. The amendment to Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information limits the possibility of charging for re-use, expands the circle of public sector authorities for re-use (e.g. also to museums, libraries and archives), defines an obligatory framework for providing legal protection and promotes the provision of information in machine-readable and open formats. As a consequence of the changes, the Slovenian legislative framework will have to be adapted in the upcoming year (the amendment

to ZDIJZ), and later all these changes will have to be effectively implemented in practice.

3. Slovenia will have to devote more attention to the promotion of greater proactive transparency and good practice in the area of open data re-use (more information should be available and forwarded without applicants' requests, thus enabling more frequent re-use), because the development and full exploitation of the opportunities, that the re-use of such information brings, are underexploited (also economic) potential in Slovenia.

4. Guidelines and good practice in the area of copyright regulation in the public sector should be prepared and, consequently, good practice in the field of public information access and re-use should be promoted.

5. The strengthening of cooperation with non-government organisations and responsible authorities and with this the raising of awareness of the significance of the right of access to public information remain very important areas. Merely effective and transparent operation of responsible authorities together with active cooperation with non-government organisations, which have to play the part of litmus paper and point out the weaknesses in key areas of the operation of society, can lead Slovenia to the next level of development in the area of government and public administration transparency. This means that enabling ease of access to the widest possible range of freely accessible public information would become a primary goal in itself and not just a legal obligation in the mind of both applicants and responsible authorities.

1.7. The Information Commissioner's assessment of key challenges in the field of Privacy over the next five years

1. One of the key challenges in the field of personal data protection is above all the European legislative framework reform. The 1995 Directive definitively no longer offers the right answers to the challenges represented by the internet, global information exchange and trends, which include "internet matters", cloud computing and "big data". The activities of the Information Commissioner will largely depend on the new regulations.

2. Among key challenges are difficult issues regarding personal data protection and public access to personal data. With digitalised media archives, in addition to the possibilities, offered by internet browsers and cloud computing, dilemmas arise regarding the admissibility of (purpose of) data use on-line and the right to be forgotten or erased.

3. In the future, profiling will definitely be an area, which will require greater attention from privacy supervisors. Both the private and public sector collect more and more data, which, with automatic processing can lead to decisions with serious consequences for an individual. It is possible that, more and more, algorithms will guide our lives, and that the boundaries of our privacy and with this our freedom, will be more and more limited.

4. The question of the balance between freedom and control, which is reflected in many disputes during the introduction of new monitoring technologies and competences, which greatly violate basic human rights, will remain an important area. With the introduction of new technologies, such as biometric face recognition systems, automatic license plate recognition systems, RFID chips, drones, etc., finding the right balance will require appropriate involvement of privacy supervisors. It should be mentioned that it will be extremely important, how successfully they will be able to show and defend the relationship between privacy and freedom.

5. However, the most important key challenge will be how, from personal data, a benefit to society can be derived while at the same time maintaining personal data protection. The processing of medical, location, transaction and other personal data can significantly contribute to solving many issues we are facing (e.g. pollution, traffic problems, etc.), but it will be essential that we will be able to extract the most from this data in a way that maintains its personal character. Both personal data and public information are currencies of the information age.

2 INFORMATION COMMISSIONER

2.1. Competences of the Information Commissioner

On 30 November 2005, the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act (ZInfP) with which a new and independent state authority was established as of 31 December 2005. The Act merged two authorities, namely the Commissioner for Access to Public Information, which had the status of an independent body, and the Inspectorate for Personal Data Protection, a constituent body within the Ministry of Justice. With the implementation of ZInfP, the Commissioner for Access to Public Information continued its work as Information Commissioner, which also assumed responsibility for the inspectors and other employees of the Inspectorate for Personal Data Protection, as well as its equipment and other resources. At the same time, responsibility was assumed for all outstanding matters, archives and records kept by the Inspectorate for Personal Data Protection. Thus the competences of the office that had previously been responsible for the unimpeded access to public information changed considerably and expanded to encompass the legal field of personal data protection. In this manner, the Information Commissioner became a national supervisory authority for personal data protection commencing its operations on 1 January 2006.

Independence of the Information Commissioner is guaranteed in two ways. First is the procedure of appointment of the Commissioner, who as a public official, is appointed by the National Assembly of the Republic of Slovenia on the proposal of the President of the Republic of Slovenia. Second is by ensuring financial independence, with the work of the Information Commissioner financed from the budget of the Republic of Slovenia and funds allocated by the National Assembly based on the proposal of the Information Commissioner.

On 21 May 2009, following a proposal by the President of the Republic of Slovenia, dr. Danilo Türk, the National Assembly confirmed Nataša Pirc Musar for a further mandate which will expire in July 2014.

The Information Commissioner carries out statutory duties and responsibilities in two areas:
1. in the field of access to public information,
2. in the field of personal data protection.

In the field of access to public information, the Information Commissioner has the role of an appellate authority competent to decide on appeals against an authority's decision to deny or refuse an applicant's request or in any other manner violate the right to access or re-use of public information, and also, with regard to appellate proceedings, to supervise the implementation of the law regulating access to public information and the regulations adopted thereunder (jurisdiction is laid down in Article 2 of ZInfP).

In the field of access to public information, the Information Commissioner also has competences as determined by the Media Act (Article 45). According to ZMed, a responsible authority's negative response to a question posed by a representative of the media shall be considered as a rejection of the request. The non-responsiveness of a responsible authority in such an instance is an offence, as well as grounds for a complaint. The Information Commissioner makes a decision with regard to a complaint against a rejection decision, pursuant to the provisions of the Access to Public Information Act.

In the field of personal data protection, the Information Commissioner has, under the Personal Data Protection Act and Article 2 of ZinfP, among others, jurisdiction to:
1. carry out inspections regarding the implementation of ZVOP-1 and other regulations governing the protection or processing of personal data (consideration of complaints, appeals, messages and other applications referring to suspected violations of the law, and carrying out planned preventative inspections of data controllers in the public and private sector) (jurisdiction is determined by Article 2 of ZInfP);
2. decide in relation to complaints made by individuals when the data controller denies the request of the individual regarding their right of familiarisation with the requested data, printouts, lists, access, certificates, information, clarifications, transcriptions or copying in accordance with provisions of the law that regulate the protection of personal data (jurisdiction is determined by Article 2 of ZInfP);
3. conduct minor offence proceedings in the area of personal data protection (expedited

procedure);

4. publish, on the website and in any other appropriate manner, preliminary opinions on the compliance of draft laws and other regulations, with the law and other regulations pertaining to the protection of personal data, and requests for constitutional reviews of regulations (Article 48 of ZVOP-1), publish court decisions relating to personal data protection and non-binding opinions, interpretations, observations and recommendations concerning personal data protection in individual areas (Article 49 of ZVOP-1).

The Information Commissioner also functions as a minor offence authority, responsible for the supervision of the implementation of ZInfP, ZDIJZ as regards the appeal procedure and the provisions of Article 45 of ZMed and ZVOP-1.

Under Article 2 of ZInfP, the Information Commissioner can file a request before the Constitutional Court of the Republic of Slovenia for the review of the constitutionality of a law, regulation, or general act issued for the exercise of public authority if a question of constitutionality or legality arises in connection with proceedings it is conducting, in both the field of access to public information and personal data protection.

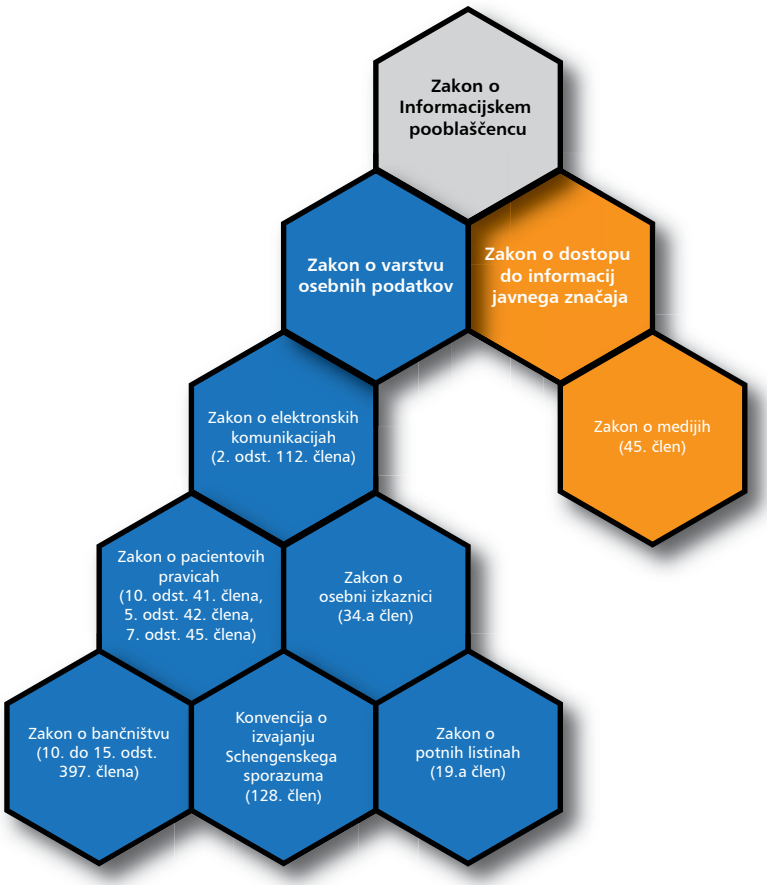
With the entry of the Republic of Slovenia into the Schengen Area, the Information Commissioner also assumed responsibility for supervision of the implementation of Article 128 of the Convention Implementing the Schengen Agreement and is an independent supervisory body responsible for supervising the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

Since 2008, the Information Commissioner has competences under the Patient Rights Act, the Travel Documents Act, and the Identity Card Act. In 2009, the Information Commissioner also gained competences under the Banking Act.

Competences which the Information Commissioner had under the Electronic Communications Act were increased with the adoption of legislation at the end of 2012 extending its responsibilities, among others, to:

- carrying out inspections to monitor the implementation of the provisions of Article 149 of ZEKom-1, which regulates internal procedures following requests from competent authorities for access to users' personal data on the basis of sectoral laws;
- carrying out inspections, at least once a year, covering the processing of data specified in Article 153 of ZEKom-1, which sets out the conditions and procedures for the transmission of traffic and location data in case of the protection of life and limb of the individual;
- carrying out inspections to monitor the implementation of the provisions of Article 166 of ZEKom-1, which regulates the transmission of stored data to competent authorities;
- carrying out inspections of the storage of traffic and location data generated or processed in connection with the provision of public communications networks or services, as provided for in Articles 162-168 of ZEKom-1, with the exception of the provisions of paragraph 4 of Article 165 of ZEKom-1 (in accordance with Article 169 of ZEKom-1);
- in the area it monitors, the Information Commissioner makes decisions regarding violations of ZEKom-1 and pursuant to regulations issued thereto, as a minor offence authority, in accordance with the legislation governing minor offences (Articles 232-236 of ZEKom-1).
- In 2013, the Information Commissioner's competences were extended following an amendment to the Consumer Credit Act. Article 36 of ZPotK-1 provides that the Information Commissioner shall carry out monitoring of (money) lenders.

Figure 1: Competences of the Information Commissioner

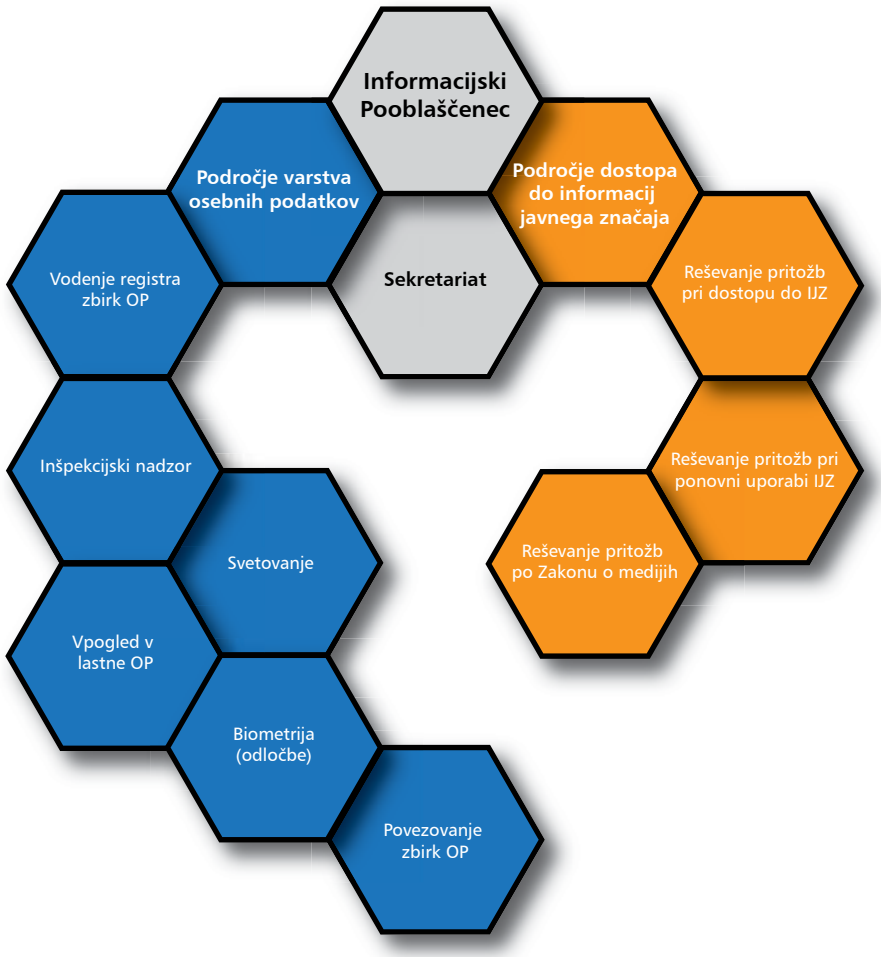


2.2. Organisational structure of the Information Commissioner

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

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

Figure 2: Organisational Chart of the Information Commissioner.



At the end of 2013, the Information Commissioner had 32 employees, of which three were employed on a temporary basis, substituting for absent employees.

The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia based on the financial plan proposed by the Information Commissioner (Article 5 of ZInfP). In the 2013 fiscal year, total funds allocated by the National Assembly to finance the operations of the Information Commissioner amounted to EUR 1,291,210.00 (EUR 1,052,017.10 for wages and salaries, EUR 210,652.18 for material costs, and EUR 28,540.72 for investments).

Based on a budget reallocation decision, EUR 3,800.00 was reallocated from the Ministry of the Interior in October, to cover the Information Commissioner's business travel costs, following her appointment among a group of five experts to the ad hoc EU-US working group. At the end of 2013, the funds allocated for material costs amounted to EUR 214,452.18 and total funds

amounted to EUR 1,295,010.00.

In 2013, the Information Commissioner's total earmarked funds and donations to participate in projects funded by the European Union amounted to EUR 104,527.88 (funds transferred from 2012 amounted to EUR 53,211.36 and funds received in 2013 amounted to 51,316.52 EUR).

Due to budgetary constraints and austerity measures adopted by the Slovenian government in 2013, the Information Commissioner has limited employee training, significantly limited participation at international meetings, and carefully and very restrictively used financial resources for material costs, investments and wages. In 2013, the Information Commissioner significantly reduced its property rental costs, when in March 2013 it moved its offices to premises owned by the Republic of Slovenia at Zaloška 59 in Ljubljana and which had been allocated to the Information Commissioner following a Government decision in February. The Information Commissioner also significantly reduced the cost of issuing publications, students' work and other services.

At the end of 2013, the Information Commissioner's total available funds amounted to EUR 1,399,537.88. Given the above and the additional restrictions on general domestic budgetary funds (reduced to 93%) at the end of 2013 the use of budgetary resources amounted to EUR 1,380,117.83.

The Information Commissioner transferred earmarked funds and donations in the amount of EUR 7,063.62 to the 2014 budget (EUR 6,717.20 of donations and EUR 346.42 of other reserves).

3 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

3.1. Activities in the field of Access to Public Information in the Republic of Slovenia

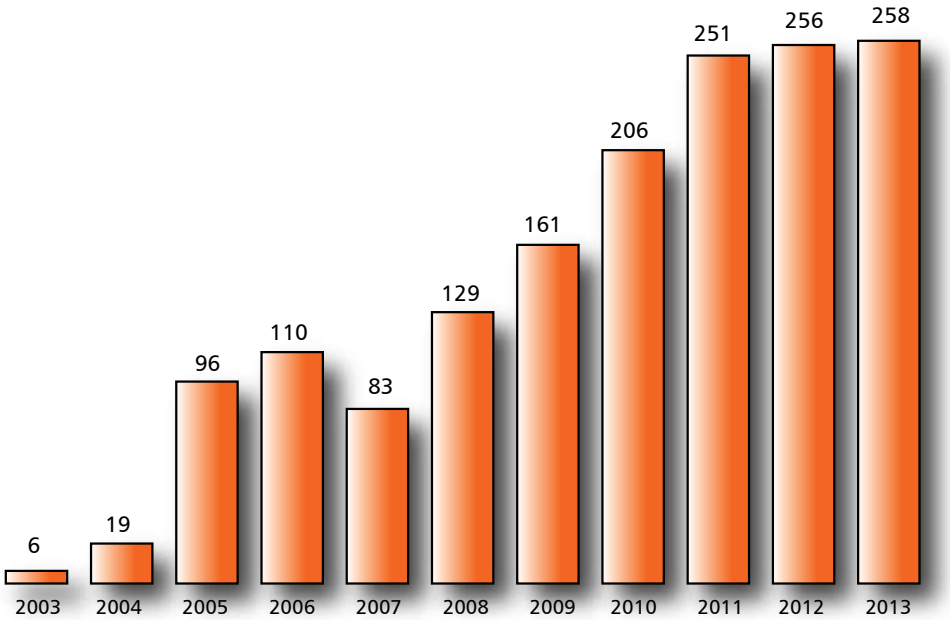
The right to access public information was ensured by legislators in the Constitution of the Republic of Slovenia. The second paragraph of Article 39 of the Constitution determines that everyone has the right to obtain information of a public nature in which they have a well-founded legal interest under law, except in circumstances as provided by the law. This right is further regulated in the Access to Public Information Act (hereinafter: ZDIJZ), 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, bearers of public authority, and public service contractors. The Act includes the public interest test.

In 2013, the Information Commissioner received 610 appeals, of which 271 were against decisions refusing requests, while 339 were against the non-responsiveness of first-instance authorities. In appeal proceedings against decisions in which responsible authorities rejected requests for access to or re-use of public information, the Information Commissioner issued 258 decisions (of which 53 cases had been submitted to the Information Commissioner prior to 2013, and one case in which it re-evaluated its decision following a judgement of the Administrative Court). Four applicants withdrew their appeals, two appeals were dismissed by the Information Commissioner, and in one case matters were combined. In processing these appeals, 54 so-called in camera examinations were carried out by which the Information Commissioner establishes the actual state of the documents held by the responsible authority.

The following decisions were issued by the Information Commissioner:

- in 115 cases it dismissed the appeal as unfounded;
- in 89 cases it granted partial access to information;
- in 36 cases it granted the appeal in favour of the applicant;
- in 17 cases it returned the matter to the first-instance authority for reconsideration;
- in one case the appeal was dismissed on procedural grounds.

Figure 3: The number of decisions issued in relation to access to public information from 2003 to 2013.



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 (104 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 and/or data deemed to be a trade secret in accordance with the legislation regulating commercial companies (34 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 and activities of the authority (33 cases);
- whether a violation of procedural rules occurred (26 cases);
- whether the information requested relates to the work and personal information of public servants and officials (19 cases);
- whether authorities charged the correct fees for providing public information (18 cases);
- the issue of a decision in procedures in which the applicant requested documents related to public procurement procedures (16 cases);
- whether the public interest in disclosure outweighs the public interest or the interest of other persons in restricting access to the information requested (16 cases);
- whether it is the field of work of the authority (13 cases);
- 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 (11 cases);
- whether the information requested pertains to data that was obtained or compiled because of or relating to a criminal prosecution or minor offence proceedings, whose disclosure would be harmful to the course of such proceedings (10 cases);
- the issue of a decision in procedures in which 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 request (10 cases);
- whether the authority to whom the request for access to public information was addressed is in fact responsible under the first paragraph of Article 1 of ZDIJZ (9 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 detrimental to the course of such proceedings (9 cases);
- whether the information requested is protected by copyright legislation – in such instances the applicant is offered familiarisation with the information by allowing them to view it (7 cases);
- whether the information requested pertains to data that was obtained or compiled on the basis of administrative proceedings, and the disclosure of such would be detrimental to the course of such proceedings (6 cases);
- whether the re-use of certain public information is involved (6 cases);
- whether the information requested 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 (5 cases);
- whether the information requested pertains to data classified as confidential in accordance with legislation regulating classified information (2 cases);
- whether archival information is involved (2 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 ZDIJZ (1 case);
- whether European Union law is involved (1 case);
- whether a violation of rights according to ZDIJZ is involved (1 case);
- whether the case concerns environmental information (1 case);
- the proactive publication of information (1 case);
- whether the information requested pertains to data whose disclosure would result in a
- violation of the confidentiality of individual data on reporting units in accordance with the law regulating national statistics (1 case).

The Information Commissioner handed down decisions in appeals filed following access to public information being denied in which the following groups of responsible authorities were involved:

- state authorities (122 cases), including ministries, constituent bodies and administra-

tive units (104 cases), the courts, State Prosecutor's Office and State Attorney's Office (18 cases),
- public funds, institutions, agencies, public service contractors, and bearers of public authority (80 cases),
- municipalities (55 cases).

One appeal referred to a legal entity in the private sector, however it was established that the entity was not responsible under ZDIJZ.

172 appeals were submitted by natural persons, 62 by private sector legal entities, 15 by journalists and 9 by public sector legal entities.

In 2013, the Information Commissioner received 339 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 27 cases the Information Commissioner rejected the appeal due to premature or incomplete applications, eight applicants withdrew their appeals because they received the requested information, in 11 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. In 2013, 23 appeals were filed with the Administrative Court against decisions of the Information Commissioner (i.e. against 8.9% of the decisions issued). As two of the plaintiffs subsequently withdrew their appeals, the share of decisions against which appeals were filed is slightly lower, at 8.1%. The decision-appeals ratio has been declining for the last few years: In 2011, appeals were filed against 13.1% of the decisions issued by the Information Commissioner, and in 2012 against 10.5%. The relatively small ratio of such appeals 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 various authorities and applicants. In 2013, the Administrative Court issued 33 judgements in relation to appeals filed against decisions of the Information Commissioner in which it decided to:
- dismiss the appeal as unfounded (17 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 (10 cases),
- partially grant the appeal, that is partially reverse the contested decision and return it to the Information Commissioner for reconsideration, rejecting or dismissing the remaining part of the decision (1 case),
- stop the proceedings due to the withdrawal of the application (2 cases),
- dismiss the appeal on procedural grounds (2 cases),
- partially dismiss the appeal as unfounded and partially reject the appeal on procedural grounds (1 case).

In 2013, no revision of Administrative Court decisions was successfully filed with the Supreme Court.

In 2013, the Supreme Court decided on a revision and appeal against a judgement and decision of the Administrative Court, however the Court rejected the request for a revision on procedural grounds and dismissed the appeal against the decision as unfounded.

In 2013, the Information Commissioner received 622 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 2013, two minor offence proceedings were initiated:
- due to a violation of the third paragraph of Article 39 of ZDIJZ, wherein, despite calls from the Information Commissioner, the responsible authority had failed to provide the requested public information to the applicant or issue a decision on their request,
- due to a violation of the first paragraph of Article 15 of ZInfP, wherein an authority failed

to forward documents required by the Information Commissioner for the adoption of a decision in appeal proceedings.

3.2. The Most Significant Cases and Precedential Cases in different areas

Internal operations of a public authority

The Information Commissioner partially annulled Decision No. 090-40/2013/4 of 13 March 2013 and requested that the Ministry of the Interior supply part of an application that it had forwarded to the inter-ministerial commission pursuant to the Decree on Defence and Confidential Procurement which contained information on the purpose and subject of the procurement.

In that part of the decision against which the applicant appealed, the ministry had made reference to point 11 of the first paragraph of Article 6 of ZDIJZ. Pursuant thereto, documents or parts of documents are protected in as far as they are intended for internal communication or communication between authorities and where it is asserted that they cover the tactics and methodology of police work, technical capability, use of special technical devices, internal general instructions for conducting investigations, instructions for identification of proceedings as well as sensitive internal instructions, plans specifying the means, tactics and methodology of collection and implementation of various kinds of surveillance and investigation. Making all these documents public would jeopardise the critical, innovative and efficient work of the authority as well as threaten the efficient investigation of crimes and the safety of investigators. According to the authority, the disclosure of information pertaining to the purpose and subject of the procurement would be detrimental to work efficiency and the performance of tasks carried out by the police.

Firstly, the Information Commissioner established that the requested information had not arisen in connection with the internal operations of the authority. The information arose during the procedure carried out pursuant to the Decree on Defence and Confidential Procurement wherein the authority, which needed to obtain the consent of the inter-ministerial commission referred to in Article 5 of said Decree in order to effect a procurement, was required to state the subject and purpose of the procurement in writing, detailing the facts and reasons so making the purpose of the procurement unequivocally clear, which key safety issues of the Republic of Slovenia need to be protected during the procurement and which special security measures need to be employed. Such an application is not intended for the internal operation of the authority but represents an external communication foreseen in effect by the Decree on Defence and Confidential Procurement. Internal operations of the authority could be argued in this instance if they had still been coordinating internally on the subject and purpose of the procurement which would suggest an approach for solving technical questions, exposure to specific problems, and the authority's process of decisions making. During the phase when the authority filled in the application and forwarded it to the inter-ministerial commission, it cannot be said that the information was being managed by the authority in an informal way for internal needs, but in fact, as required by and in accordance with the Decree on Defence and Confidential Procurement. The application in question is connected with confidential procurement but the document does not carry a classified label in accordance with the Classified Information Act. The application form includes instructions that the applicant authority shall not, as a rule, mention classified information in the application; if however it does, the application shall be labelled in accordance with ZTP. The nature of such a document clearly indicates the principle that the information contained therein is not connected with internal operations of the authority as it does not disclose its internal thinking but is a typical example of "external activities" which help the authority exercise its powers in relation to procurements needed for its work.

The requested information would not even pass the damage test from point 11 of the first paragraph of Article 6 of ZDIJZ as the authority, carrying the burden of proof, did not attest that disclosure of the requested information would disturb its operations or activities. The

position of the Administrative Court of the Republic of Slovenia was that the burden of proof, in relation to the reasons for disturbances in its operations, is on the authority and the standard of proof "the disclosure would cause disturbances" is a standard of proof "beyond doubt" and not merely a "probability" (Judgement no. I U 1176/2010-12). The Information Commissioner agrees with the authority that the disclosure of certain information on how the authority is equipped with technical resources could jeopardise the authority's work, however, in this case, the information requested does not disclose such data. The information in question identifies the authority's needs in general in regard to technical equipment on the basis of which it is difficult to determine specifically which equipment is the subject of the procurement, otherwise the application would have been labelled with an appropriate level of confidentiality. On the basis of the information which is the subject of the assessment, it is impossible to establish the technical capacity of the procurement, also, it is impossible to establish in which cases, with which method, and with which work tactics the authority could use the equipment. Speculation is always present but it cannot be the reason for withholding the information. On several previous occasions, the authority itself explained the disposal and use of some equipment to the media as it probably assessed that with this kind of data its work could not be jeopardised. There is no objective reason to treat the general information on the subject of the procurement, which is requested in this case, differently. Even if a procurement is confidential, it still uses public funds. The public therefore has a legitimate interest in having access to information on how taxpayers' money is being spent and whether the state uses public funds economically and in accordance with the law. The Commissioner concluded that in respect of the requested information, the claimed exemption did not exist.

Does the document exist?

With its Decision No. 090-15/2013/6 of 11 March 2013, the Information Commissioner rejected an applicant's appeal against a decision of the Office of the Prime Minister of the Republic of Slovenia, which as the responsible authority had refused the applicant's request to access e-mails, on a specific topic and in a specific time period exchanged between the Office of the Prime Minister and the offices of two specific Ministers.

The authority rejected the applicant's request, stipulating that it did not have the requested electronic correspondence nor would it have access to it if it existed.

The Information Commissioner ascertained that the authority indeed did not have the requested information. Even though the Prime Minister and the two Ministers exchanged correspondence on the topic that interested the applicant, the responsible authority was not in possession of the documents and as such did not have them at its disposal, furthermore it did not have a legal basis to acquire them. The provisions of the Decree on Administrative Operations stipulate that e-mails are primarily used for official purposes. Public employees are required to appropriately record e-mails that are sent to their e-mail address (and not to the official e-mail address of the authority) in non permanent archival records. Neither the law nor the Decree foresee sanctions for an employee who does not fulfil this requirement, further all e-mails that are received or sent from a public employee's electronic mailbox are not automatically deemed as official or work related and in the authority's possession. To a lesser extent the Decree also allows the possibility of using e-mails for private purposes.

The authority has no jurisdiction to examine electronic mailboxes of individual public servants or officials (for example name.surname@gov.si). By entering into an employment contract in the public sector, public servants and officials do not fully renounce their privacy in the workplace. Under the applicable legislation neither the authority nor the Information Commissioner have jurisdiction to examine the electronic mailboxes of public servants (or public officials) to determine whether a work related e-mail should have been recorded in the system of archival records but was not. To do so would be a violation of the constitutional right to communication privacy of the public servant or public official. Article 37 of the Constitution of the Republic of Slovenia ensures confidentiality of letters and other means of communication. Only the law can stipulate that, based on a court's decision, and for a specified period of time, the protection of confidentiality of letters and other means of communication and the integrity of an individual's privacy is not respected, if this is necessary for the implementation of or during the course of criminal proceedings or for national security. From the above mentioned decision several conditions emerge

which must be met for the intrusion into the confidentiality of letters and other means of communication to be justifiable when there is also an invasion of privacy involved. These conditions are not met in this case. The decision of the European Court for Human Rights in the case of Copland against the United Kingdom should also be noted. In this case, the Court recognised a broad range of privacy rights of the employee and judged that the employer unjustifiably invaded her privacy. The key element of the judgement is that the employee was not warned in advance when and in which cases the employer could examine her e-mails.

The Information Commissioner believes that the responsible authority provided all documents it had available in relation to the content that the applicant was interested in (a record of Lotus Notes System for a specific case and explanations on certain matters). However, this documentation does not include documents which are the subject of the applicant's request. This case did not meet the first condition from the first paragraph of Article 4 of ZDIJZ which provides that public information is only information which an authority already has available or has in its possession. The Information Commissioner thus concluded that the applicant's request could not be granted.

Public interest test, public servants, internal operations

The Information Commissioner partially annulled Decision No. 090-49/2013/5 of 6 May 2013 and ordered the Commission for the Prevention of Corruption, as the responsible authority, to supply an audio recording of a discussion with the president of a parliamentary party, which was made during the preparation of the Final Report on the Inspection of the Financial Condition of Parliamentary Party Presidents (hereinafter: Final Report).

When it rejected the application, the authority referred to entitlement to an exemption for the protection of court proceedings. While the authority was deciding on the request for access to the document in question, the Administrative Court had not yet reached a decision in an action filed against the Final Report.

The Information Commissioner did not follow the arguments of the responsible authority. In the appealed decision, the responsible authority did not explain how the content of the requested recording was different from content which had already been made public and related to part of the Final Report referring to a particular president of one of the parliamentary parties, nor what adverse effects the disclosure of this part of the recording would have on the proceedings before the Administrative Court. It is also important to note that the Court rejected an application for interim measures to remove the Final Report from the authority's web page. This means that the Final Report remains publicly accessible as the Court did not consider that making it public would cause any harm nor endanger the course of the judicial proceedings in question. The Information Commissioner concluded that the claimed exemption did not exist.

Furthermore, the Information Commissioner determined that this was an internal document which could represent an exemption to publicly accessible information based on protection of the internal operations of the responsible authority. The fact is that the authority's meetings are not public and take place in the spirit of confidentiality and (in consideration of the applicable laws) it is expected that the content of such meetings remains confidential. The disclosure of such documents could cause disturbances to the authority's work as it is necessary to be aware that the participants at such hearings would not furnish all the answers or state all the facts if they knew that their entire hearing would be made public. Nonetheless, the requested recording must be made public as there is a predominant public interest in doing so. In this case, the Final Report on the Inspection of the Financial Condition of Parliamentary Party Presidents had important and far reaching consequences for the whole of the Republic of Slovenia. The publication of the Final Report led to a change of government, there were a number of public discussions on this topic, including a broad public discussion on the integrity of the public officials in question and their attitudes to the authority and its findings. The Final Report presents some actual findings while the requested audio recording provides further information on how proceedings were conducted before the authority's senate, namely, whether certain of the authority's findings were presented to the public official, what his subjective attitude towards these

findings was and also what his subjective attitude towards the authority as an independent public authority was. In relation to the Final Report, there was wide public debate on the question of political responsibility of public office holders and in particular relating to a specific public official who is the Mayor of the largest city in Slovenia. This public official often made statements about the contents of the Final Report and the proceedings before the responsible authority. There were reproaches made in public that the public officials being investigated were not given the opportunity to cooperate in the proceedings nor the possibility of supplying all evidence. This Final Report raises an important question of political responsibility of public officials, an open debate on this question leads to a heightened political culture in Slovenia, further develops political responsibility, strengthens the integrity of public officials and public servants, and encourages responsible conduct of proceedings before national authorities and transparent decision-making. The information contained in the requested recording is important for a comprehensive understanding of the Final Report as well as for having an open public debate on the integrity of public officials in this particular case and in general, and a debate on transparent conduct of proceedings and decision-making before such an important national authority as is the one in this case.

Having regard to the foregoing, the Information Commissioner granted the appeal of the applicants and decided in this case, that even though the requested audio recording represents an exemption to freely available public information, the disclosure of such information is in the public interest.

Confidential data, withdrawal of security classification

The Information Commissioner's Decision No. 090-157/2010/55 of 26 April 2013 was the last of the decisions dealing with an appeal filed against two decisions of the National Assembly following the request of the applicant for access to documentation connected with the so-called "arms trafficking" events, that is, connected to events that took place twenty years earlier and which the responsible authority had in its possession as part of the investigating commissions which had been dealing with these events.

The subject of this supplementary decision is the documentation which the responsible authority has in its possession but originated from other authorities (such as SOVA, the Office of the President of the Republic of Slovenia, the Government of the Republic of Slovenia). Part of this documentation does not have security classification or rather had its security classification withdrawn, but it contains certain protected personal data which the responsible authority must conceal before supplying such documents to the applicant. With regard to documents which are labelled with a security classification, the Information Commissioner decided as to whether they were appropriately classified in accordance with ZTP and whether they represent an exemption to free access. According to ZTP, confidential data is any data that cumulatively fulfils the material and formal criteria. The material criterion includes two aspects. The first aspect is that the disclosure of such data causes or could cause certain damage, while the second aspect is in relation to the damage to an exhaustive list of areas of interests for the country (public security, defence, foreign affairs, intelligence and security activities of national authorities in particular the damage to their systems, equipment, projects and plans or scientific, research, technological, economic and financial matters which are important for these interests). Both material elements are reflected in the formal criterion for confidential data. Data can only be classified as confidential if it meets the following three conditions: data was classified as confidential by an authorised person; there must be a written evaluation on the possible adverse effects which could arise from the disclosure of such data (the authority which attached a security classification to data keeps the evaluation, which includes the designation of the protected data and an assessment of the importance and intensity of the possible adverse effects, as an attachment to the document); and the document containing the confidential data must be appropriately labelled as confidential.

The legislator linked the security classification of CONFIDENTIAL with adverse effects, the disclosure of such information could seriously damage the security or interests of the Republic of Slovenia. The label INTERNAL is linked with the damage that the disclosure of information could cause to the operations or implementation of an authority's work. As the concept of "serious damage to security or interest" is not determined by the law, it is the

responsibility of the authority, which used this judiciary rule to conceal information from the public, to determine its content, namely, to indicate how the disclosure of the information could seriously damage the country's security or interest. The Information Commissioner determined that the written assessments of possible adverse effects in this case did not meet this condition. In the written assessment of possible adverse effects, the originators of the documents only paraphrased the existing law but did not give factual explanations or clarification on how the disclosure of the requested documents labelled CONFIDENTIAL could seriously damage the security or interests of the Republic of Slovenia or how the disclosure of documents labelled INTERNAL would adversely effect the operations or the implementation of the authority's work. From the written assessments of adverse effects it is also not clear to which of the protected areas the requested documentation refers. Moreover, for SOVA's documents labelled INTERNAL, it was claimed that their disclosure would damage the agency's reputation which definitely contradicts the purpose and goals of ZTP, which determines that confidential data is data whose importance is such that its disclosure to an unauthorised person would or obviously could have detrimental effects for the security of the country or its political or economic interests in certain defined areas, which has nothing to do with the agency's reputation. Thus it is unclear which legally determined areas the disclosure could endanger. An approximate assessment, based only on the legal norm, is an illegitimate use of the institute of confidentiality as it is impossible to determine the reasons that dictated the decision of the originators of the documents in labelling them CONFIDENTIAL and INTERNAL, which is exactly what the law in a democratic society calls for with a written assessment of adverse effects. The originators of the documents could only assert the occurrence of damage on an abstract level without being specific. It is therefore impossible to determine whether the claimed adverse effect could even occur. Given the fact that the events mentioned in the requested documents occurred two decades ago and that there had been many debates on the topic in the media, that several books had been published and a vast majority of the documents had already been made public, the damage which was only approximately forecast by the originators is therefore completely speculative or it would have already been caused by access to documents published earlier with content covering identical areas as the current documents labelled as confidential, but no damage was caused, nor did the originators make any reference to it. These documents have "a historical value" which, besides offering a complete picture of the (now concluded) events, can no longer damage the security or interests of the Republic of Slovenia, which is what the institute of confidentiality is designed for. It follows that there was no reason for these documents to be labelled with a security classification as the material condition for the existence of confidential data was not met. From the point of view of the assessment of importance and intensity of the possible adverse effects, the formal criterion was not met either. The exemption under point 1 of the first paragraph of Article 6 of ZDIJZ did not apply.

Taking into account that the data is labelled with a security classification in contravention of the law pertaining to classified information and that the applicant explicitly demanded that the security classification be withdrawn, the Information Commissioner decided that the originators must withdraw the security classification from the documents in question and forward them to the authority which must provide them to the applicant, prior to which it is required to hide protected personal data.

Internal operations of an authority

With its Decision No. 090-22/2013/6 of 19 April 2013, the Information Commissioner annulled the decision of the National Examinations Centre, as the responsible authority, and ordered that it supply the list of schools mentioned in the Annual Report on the General Matura Examination in the chapter titled Quality analysis of the General Matura examination by schools.

The authority rejected the request of the applicant, referring to Article 18.a of the Matura Examination Act which specifies that the data from the annual analysis of the quality of the examination should not be used to classify schools. This Article was adopted with a view to prohibit any form of data processing which could lead to the classification of schools. Due to this provision, the responsible authority prepares and publishes the analysis under a code concealing the identity of schools.

The Information Commissioner determined that the requested data are freely accessible public information which do not merit exemption to free access. The nature of the requested data is not such that it could protect the internal thought processes of the responsible authority, the data do not originate from documents which would result from the authority's policy-making processes and therefore do not protect the authority's decision-making process nor would their disclosure endanger the free flow of ideas during the processes of decision-making or formulating of procedures. The authority has no competence for policy making in the area of education. The requested documents contain facts, namely a summary of data on the results of the general matura examination. Even if the requested data was related to internal operations, their disclosure could not cause the authority a level of damage which could seriously and materially endanger its operations or activities. The responsible authority could continue to carry on its tasks as specified in ZMat, including the collection and analysis of data on the matura examination.

The authority's argument that the information was only requested because it could be the subject of incorrect interpretations and conclusions, either inexact or incorrect, is unconvincing. The untrustworthiness of the requested data is not a reason for the refusal of access to this information. The authority's concerns that the public will receive untrustworthy and raw data is understandable but cannot be reason for an exemption citing internal operations of the authority. The authority always has the opportunity to offer explanations with which it can avoid any incorrect interpretations of the data. The amended Article 18.a of ZMat, to which the authority refers in this case and which stipulates that the data on students' success in the matura examination in individual schools (which is drawn from the annual analysis prepared by the authority) must not be used to classify schools, cannot be the reason for the authority's refusal to allow access to this data. This Article of ZMat only prohibits the classification of schools, it does not prohibit access to the data. From the point of view of exemptions which are stipulated in Article 6 of ZDIJZ, the (new) Article 18a. does not change the actual situation concerning the requested information. An important fact is that individual data which the applicant requested would be considered freely accessible public information (and clearly no damage would occur if the applicant acquired them individually from each school). It is therefore not acceptable that the same data would be considered exempt to free access only because they are in the form of a list. It is essential that in a procedure pursuant to ZDIJZ an individual document is always judged as such, without regard to the fact of what the applicant, for example, with the help of combining data from the requested document with other freely accessible information, could find out, what conclusions could be drawn and whether these would in fact be the conclusions of the applicant. The requested document only includes a list of names of schools which does not represent any exemption from free access to public information, therefore the responsible authority must supply it to the applicant.

Environmental data

With Decision No. 090-66/2013/9 of 29 May 2013, the Information Commissioner partially annulled the decision of the Radioactive Waste Management Agency and ordered it to supply the Manual for Project Management of Low- and Intermediate-Level Radioactive Waste, ensuring that protected personal data is hidden.

The authority refused the applicant's application and stated that the requested manual is of an internal nature and defines the authority's internal procedures. Its content is part of the authority's know-how and as such a trade secret. The manual does not include environmental content and covers only processes and procedures that have to be carried out in relation to the project management of a waste repository.

The Information Commissioner invited the company which prepared the requested manual to be a third-party participant in the appeal proceedings but it did not respond to the invitation. The Information Commissioner then considered whether the requested document could be an exemption under point 2 of the first paragraph of Article 6 of ZDIJZ and found that no trade secret existed under the subjective criterion (the first paragraph of Article 39 of the Companies Act) as there is no rule determining which data are considered a trade secret for the requested document. The requested manual does not pass the trade secret damage test as specified in the second paragraph of Article 39 of ZGD-1 (according to the objective criterion). It should be emphasized that only data which represent a

competitive advantage for a company can be considered a trade secret. The authority does not market the requested manual, but carries out a public service of radioactive waste management regulated by the Ionising Radiation Protection and Nuclear Safety Act. It does not have competition in this area, nor is it possible to talk about the possible damage to the competitive position of the authority. The work of the authority is financed by public funds (funds of the NEK Fund), therefore data originating from this work cannot be a trade secret as this would contravene the third paragraph of Article 39 of ZGD-1 in relation to the third paragraph of Article 6 of ZDIJZ. That this is not data, the disclosure of which could cause significant damage to the market position of any other subject is confirmed by the fact that the company which prepared the document did not declare third-party participation in the appeal proceedings.

In this case, it is impossible to talk about an exemption pursuant to point 9 of the first paragraph of Article 6 of ZDIJZ, as the requested manual is no longer in the phase of compilation nor is it the subject of consultations within the authority. This document is a comprehensive and technically elaborate document which may only be a version of the manual which will actually be used during the various phases of the waste repository project, however, this does not change the fact that it is a finalised document. Concerning the damage that would be caused due to the public's misunderstanding of the document's contents, the burden of proof is on the authority which argued this element of the claimed exemption only on an abstract level. Concerns about possible erroneous interpretations can be overcome in ways which do not restrict access to the requested information, for example with explanations. Introducing the requested document to the public could even help the public to better understand the requested document and enable easier cooperation in the suitable organisation of the waste repository.

Even if the requested manual could be defined as one of the exemptions from free access to information, the public should be granted access on the basis of the third paragraph of Article 6 of ZDIJZ, as this data concerns the use of public funds and the environment. The compilation of the requested manual and the waste repository project, which is the subject of the manual, are financed by public funds. The data in the requested manual includes data on low- and intermediate-level radioactive waste (hereinafter LIRW) and data which is directly and intrinsically connected with this type of waste (such as the legal basis for waste management, the purpose and the goals of the waste repository, the financial framework and the products of the second phase of the project, the organisation of the project and the key processes of its implementation), and being based on real and predicted data on the LIRW in connection with the repository, cannot be separated from the data relating thereto as together they both form an inseparable whole. The manual describes the processes which will be carried out at the LIRW repository project, which could not have been formulated without the data on emissions to the environment, waste and hazardous substances in the plant. Without such data, it was impossible to determine the phases, organisation, purpose and goals of the project and consequently the financial framework. The requested document includes the processes and procedures which have to be implemented in relation to management of the LIRW repository project. It is clear that this document contains data on LIRW.

In accordance with the definitions from Article 3 of the Environmental Protection Act (ZVO-1) which, among basic principles, determines the principle of cooperation and the principle of public access, the Information Commissioner determined that the LIRW data is environmental data relating to waste because the producer of these specific substances or objects or other person who has them in their possession would discard them. In this particular case, the waste can be more accurately described as radioactive waste which is defined in ZVO-1 as waste, which due to certain radioactive properties.as set out in the regulations on the protection against ionizing radiation, is classified among radioactive waste. These substances emit ionizing radiation, as such their impact on the environment can be characterised as emission. LIRW must also be defined as a so-called hazardous substance.

The requested manual therefore contains data on hazardous substances, waste and emissions. Access to such data on the basis of the second indent of the third paragraph of Article 6 of ZDIJZ is permitted irrespective of the provisions of the first paragraph of Article 6 of ZDIJZ, which stipulates the exemptions to free access to public information. With this provision, ZDIJZ sets a statutory requirement that the overriding public interest in

the disclosure of data prevails whenever the data concerns emissions to the environment, waste, hazardous substances in a plant or data from a security report, and other data as determined by the law on environmental protection. In this way, the legislator extended the rights provided for in the second paragraph of Article 6 of ZDIJZ, as demonstrating and proving an overriding public interest is not necessary in such cases.

The Information Commissioner concluded that the content of the requested manual, based on the provisions of the second indent of the third paragraph of Article 6 of ZDIJZ, must not be exempted from free access, meaning that the requested manual is, from this point of view, freely accessible public information. The responsible authority must supply the requested manual to the applicant, ensuring that protected personal data is hidden.

Copyrighted work

With its Decision No. 090-83/2013/7 of 26 June 2013 the Information Commissioner partially annulled the decision of the Municipality of Kanal ob Soči, being the responsible authority, ordering it to supply photocopies of the recipe for Marijaceljski Cake and the purchase agreement for this recipe, ensuring that protected personal data is hidden.

The responsible authority refused the applicant's request, to forward them a photocopy of the recipe, due to existing copyright, but allowed the applicant to view it. The authority claimed that no purchase agreement for the recipe existed.

The Information Commissioner discovered that the authority was in possession of an agreement entitled "Agreement on the creation of copyrighted work" on the basis of which the requested recipe was purchased as part of the LAS Project. This agreement includes some personal data of the person with whom the agreement was concluded. With the exception of name and surname, this data is protected personal data. Information on who the authority paid budgetary funds to represents data on the use of public funds, which, based on the provisions of the third paragraph of Article 6 of ZDIJZ, cannot be exempted from free access to information. When supplying a photocopy of the agreement to the applicant, the authority must hide protected personal data.

Pursuant to Article 17 of ZDIJZ, the applicant has the right to decide how they want the requested information to be presented. The only restriction that can effect the format of the supplied information is found in the second paragraph of Article 25 of ZDIJZ which provides that the applicant may only view information protected in accordance with the act governing copyright. As the applicant wanted to acquire a photocopy of the cake's recipe, it was necessary to determine whether such a document is protected by the act governing copyright, and consequently, whether the manner in which the requested information is presented to the applicant can be restricted. In accordance with Article 5 of the Copyright and Related Rights Act a copyrighted work is an individual intellectual creation in the domain of literature, science and art, expressed in any mode, unless otherwise determined by ZASP. Five assumptions originate from this definition, existing judicial practice and legal doctrine which need to be fulfilled cumulatively so that a work can be considered a copyrighted work under ZASP. These assumptions are individuality, intellectuality or spirituality, conception, field of creativity and expression. The Information Commissioner found that the criterion of individuality was not met in this particular case. A work's individuality is a characteristic which distinguishes copyrighted work from other works protected by copyright and from works that are not protected by copyright as well as from artistic and cultural heritage which belongs to the broader public. The requirement is thus, that the work needs to have sufficient original characteristics in order for it to be considered copyrighted work. If an author, independently of another work creates his own work with individual characteristics, without copying or directly drawing inspiration from another work, the premise of the individuality of the work is fulfilled. In a work that includes only a collection of data and facts, the individuality criterion is not met and therefore it is not protected as copyrighted work. In this case, the recipe contains a list of ingredients necessary for the preparation of the cake and short instructions on how to mix and prepare these ingredients to make the desired product. With regard to originality and creativity, this recipe does not differ greatly from other similar recipes available on the internet or in a way that it would be possible to consider it as copyrighted work. The recipe is not written in a special and original manner nor does it contain graphical elements

which would distinguish it from other recipes available on the internet. Similarly, the use of words and clauses does not differ from the usual use of these elements in publicly available recipes. Copyright protects the expression of ideas and not the idea itself. The fact that the author of the recipe might think of some new ingredient to make the cake does not mean that the recipe, as an expression of this idea, fulfils the individuality criterion. To fulfil this criterion, the recipe would have to be expressed in a creative manner (in the form of a fairytale, poem, pictorially, etc.), and therefore presented in a way that differs from other recipes. In this case, there is only a standard list of ingredients and the usual instructions on how to prepare the cake. The individuality criterion of the requested recipe is not fulfilled and, consequently, it is not a copyrighted work, so there is no barrier to the responsible authority supplying it to the applicant in the form of a photocopy.

Even if it were a copyrighted work, the material copyrights of the requested document are transferred to the responsible authority with the purchase agreement for this recipe and it has the right to reproduce and distribute reproductions of the requested document. The authority's arguments that supplying a photocopy of the requested document to the applicant is not allowed, are completely ungrounded.

Trade secret, public interest test

In Decision No. 090-91/2013/9 of 15 July 2013, the Information Commissioner dismissed the appeal of the applicant against the decision of the Ministry of Finance in which it, the responsible authority, partially rejected the request for access to the proposal for the restructuring of Nova Ljubljanska Banka, d.d. (hereinafter the third-party participant).

The authority partially rejected the application on account of the protection of trade secrets of the third-party participant. The authority determined that the requested document represented a trade secret under the subjective criterion and that public interest in disclosure did not outweigh the interest of the third-party participant to restrict access to the requested document. As some parts of the requested document include data on the use of public funds, the authority granted the application in part, but rejected the request for the remaining parts of the document.

The Information Commissioner determined that the content of the requested document corresponds to the definition of a trade secret in accordance with the first paragraph of Article 39 of ZGD-1 as the document explicitly indicates that its contents are a trade secret. The third-party participant took all the necessary measures to protect data it had marked as trade secrets but this document contains some data which are public on the basis of the law and, in accordance with the third paragraph of Article 39 of ZGD-1, cannot be considered a trade secret. This is information which indicates the use of public funds, which is, regardless of being marked as a trade secret, always public information. The Information Commissioner found that apart from the data which was marked as freely available by the responsible authority, there was no other concrete information relating to the use of public funds. Simply the potential possibility of attaining additional public funds in the future does not imply the use of public funds within the meaning of the third paragraph of Article 6 of ZDIJZ.

The Information Commissioner also carried out a public interest test (the second paragraph of Article 6 of ZDIJZ). The notion of "public interest" is not legally defined, which is why it is necessary in each particular case, to determine whether the given circumstances are in the interest of the broader community and not only of an individual. It is true that people are the most sensitive when it comes to their health, life and security, but in given circumstances, the sensitivity is no less when it comes to information, connected to the state's financial operations as the consequences of these activities are often seen in or influence these values. In the past, the state as the majority shareholder of the third-party participant often intervened financially with injections of capital or other means of financing so that the bank fulfilled its legal obligations in terms of capital adequacy. There are rumours that the bank needs additional national resources. In this particular case, the subject under evaluation is the programme of restructuring which, except for the part already mentioned, does not imply the use of public funds but describes the plan on how to remedy the situation. This is data which is still in the phase of coordination with the European Commission and which demands certain conditions to be fulfilled in order to carry out a successful

stabilisation of the bank which is certainly in the public interest. According to the authority, the public interest in the disclosure of the requested documents is not as great as the public interest, that in this phase data remain unavailable to the public. If the data were made public the competition could learn of the third-party participant's weaknesses; so in this way, taxpayers' money which has already been invested in the third-party participant is protected. Given that the final decision on restructuring has not yet been taken, the Information Commissioner accepted the arguments of the responsible authority and the third-party participant that the disclosure of the requested information which is not yet a final decision, would influence the stability of the banking system in the global market and the stability of the third-party participant. The disclosure of information which is not final and is still part of the restructuring strategy would definitely influence the competitive position of the bank in the market with respect to the loss of clients (customers), the decrease of resources (deposits) and could mean worse prospects for the sale of non-strategic investments. The disclosure of information in this phase of the bank's reorganisation would achieve exactly the opposite of what was intended. It is understandable that customers and the general public are interested in whether the bank, in which the state has majority ownership, operates prudently and is still trustworthy, especially following information that has appeared in the media (controversial loans, human resources policy, purchase of vehicles...). It has to be emphasised however, that the intention of the public interest test is not to disclose something which is "of interest to the public" but to disclose what is "in the public interest". The data requested by the applicant might be of interest to the public but are definitely not in the public interest in this phase, as every country which strives to be democratic must ensure the right to free access to public information, but at the same time protect its citizens from the misuse of this right to their detriment, which is definitely true in this case, in which the disclosure of the information could jeopardise trade secrets which would then have an influence on the process of reorganisation of the banking sector which the Republic of Slovenia has an obligation to carry out.

In this case, the public interest in disclosing the requested information does not outweigh the interest of the third-party participant and the public interest, that this information remains a trade secret. The result in this public interest test is affected by its timing and the fact that the stabilisation process of the bank is still ongoing. There is no doubt that regulation of the banking system, which will meet all the demands of the Bank of Slovenia as well as the European Commission, is in the public interest as the stability of the economy in the Republic of Slovenia depends on it. Such stability also influences the general welfare and the standard of living of all its citizens. When the process is finished and the final decision on how the third-party participant will be stabilised and restructured is taken, conditions for increased transparency of the requested information will definitely be met.

Tax confidentiality, internal operations, public servants

In Decision No. 090-60/2013/17 of 5 July 2013, the Information Commissioner partially annulled the decision of the Tax Administration of the Republic of Slovenia and ordered it to supply certain parts of a report requested pertaining to an extraordinary internal audit of the work of a particular public servant in relation to the procedure for assessing tax liability of a certain taxpayer.

The authority rejected the application, referring to tax confidentiality, internal operations of the authority and personal data protection. When the data representing tax confidentiality is hidden, the requested report no longer provides the information requested by the applicant. The authority claimed that the disclosure of the requested report could cause disturbances in the authority's operations, especially concerning the efficiency of its internal control procedure as its function would be significantly diminished due to the realisation that written communication or documentation, even if it only includes probable information and suspicions, intended for management information to help implement improvements in the work process or remedy other deficiencies, can be made public.

The Information Commissioner found that even if part of the requested report needs to be hidden, it still provides information that the applicant requested. In relation to the data which are labelled as confidential, the Information Commissioner allowed the claims of the authority and dismissed the applicant's appeal in this instance as it is an absolute exemption to freely available information. The remainder of the requested report does not

contain exemptions from free access and the authority must supply it to the applicant. The requested report was certainly prepared in connection with internal operations but the disclosure of the document would not cause disturbances in the operations or activities of the responsible authority. That part of the requested report which refers to the findings about the work of a particular public servant does not contain "sensitive" internal information. In that part of the report, there is no indication of the nature of the work and methodology of the internal control activities nor findings in connection with the internal operations of the responsible authority which could influence its work or activities in the future. Given the fact that the requested report was prepared in 2011, the authority has had to remedy all the possible shortcomings that were found and it is therefore unfounded to claim that the disclosure could cause damage because the document would give taxpayers an opportunity to take advantage of the organisational and legislative deficiencies which were uncovered in the report. Given the fact that confidential tax data is hidden, the disclosure of the remaining requested data could not effect the specific tax control procedures. The disclosure of data on the findings of the internal control in relation to the activities of this particular public servant cannot seriously endanger the work processes of the authority or cause disturbances to its activities. For the existence of an exemption in relation to internal operations in accordance with judicial practice, the standard of proof "that it is very likely" that the disclosure would cause disturbances, is not enough. What is needed is the standard of proof "beyond doubt". The Information Commissioner further found that the text of the requested report did not contain personal data of the individual other than that related to her work within the authority (findings of the special internal control on the responsibilities of the public servant when carrying out tasks for which she had entered into an employment contract in the public sector, and in relation to her treatment of an individual taxpayer). Further to the provisions of the third paragraph of Article 6 of ZDIJZ, this data is not protected personal data and as such is not exempt under point 3 of the first paragraph of Article 6 of ZDIJZ. The purpose of the third paragraph of Article 6 of ZDIJZ is also to increase the awareness of public servants that their work is public and that the public has the ability to monitor their work in individual cases. Only in this way, can the responsibility and the transparency of the work of individual public servants, as well as the responsibility and transparency of the work of public sector authorities as a whole, be increased. It has to be emphasised that the purpose of exemptions under ZDIJZ (including exemptions regarding personal data protection and tax confidentiality) is to protect legitimate interests and not to conceal the possible irregularities of the work of public servants or deficiencies in the work processes of the authority as a whole.

Trade secret

With Decision No. 090-249/2013 of 20 December 2013, the Information Commissioner dismissed the appeal of a third-party participant against the decision of the Public Sector Inspectorate which had partially granted an applicant's request to access a photocopy of an agreement that the responsible authority had concluded with the third-party participant.

The authority partially granted the applicant's request to access the agreement (data hidden included the name and surname of the administrator of the agreement on the contractor's side – the third-party participant). During the proceedings the authority called on the third-party participant, which is the contracting party of the requested agreement, who opposed the disclosure citing the protection of trade secrets. The authority took into consideration the provision of the third paragraph of Article 6 of ZDIJZ and refused access to the requested agreement in that part which referred to protected personal data.

The Information Commissioner determined that all the criteria that ZGD-1 requires to define a trade secret under the subjective criterion were met in relation to the requested agreement. However, certain provisions of the requested agreement needed to be disclosed as they are public according to the law and therefore cannot be a considered trade secret under the third paragraph of Article 39 of ZGD-1. Similarly data on the use of public funds, are public on the basis of the third paragraph of Article 6 of ZDIJZ. In this case, this is data from the agreement which have a financial effect and create indirect and direct financial obligations for the authority, and data showing which services the authority received for the agreed payment and how (in which way) it will fulfil its financial obligations. Data pertaining to the time-frame of the agreement is also public – merely the amount of the contract without information on the duration of the service does not give complete infor-

mation on the level of obligations and the amount of public funds that will be used on the basis of the concluded agreement. Contractual provisions for possible changes, mutual dispute resolution and provisions that the agreement enters into force when it is signed by all the contracting parties cannot be considered trade secrets of the third-party participant. Allowing the third-party participant to unilaterally label this kind of data as a trade secret would disable public control over the legality of the authority's general agreement-making process. The agreement in question includes so-called standard contractual terms (which are part of every concluded agreement) which prove that when concluding this agreement the authority followed all the general principles of obligational law and that the agreement does not deviate from them. These terms cannot therefore represent trade secrets of the third-party participant.

Further the Information Commissioner determined that the data referring to who concluded such agreement in the name of and for the account of the authority, and who the authority's contact person is, is data pertaining to public servants or a public official (the minister), which is also freely available in accordance with the third paragraph of Article 6 of ZDIJZ. For the same reason, data on who within the authority is entitled to use the service which is the subject of the agreement, and who the administrator of the agreement is for the client – the authority, cannot be a trade secret. Involved are people, employed by the authority, who are public servants, and whose use of the portal, which is the subject of the agreement in question, is definitely related to the performance of their duties. Who the administrator of the agreement for the contractor is (the third-party participant) is not freely accessible information, therefore this data must be hidden. Data about who concluded the agreement in the name of the company is not protected information, as the signatory to the agreement is the director who is the company's legal representative. The public aspect of this data is determined by ZGD-1, the Business Register of Slovenia Act and the Court Register of Legal Entities Act. Other data which is also public according to the law and cannot be labelled as a trade secret, is the data on the agreed payment deadline which is stipulated by the law, and specified in Article 25 of the Implementation of the Republic of Slovenia Budget for 2013 and 2014 Act. The same applies to the anti-corruption clause which was included in the agreement pursuant to Article 14 of the Integrity and Prevention of Corruption Act.

The Information Commissioner concluded that the responsible authority had correctly determined that only protected personal data included in the agreement were exempted from free access and dismissed the third-party participant's appeal.

Re-use of public information

In Decision No. 090-249/2013 of 20 December 2013, the Information Commissioner annulled the decision of the Supreme Court of the Republic of Slovenia and returned the matter to the Court for reconsideration.

The applicant addressed an application to re-use published public information on decisions and communications issued in insolvency proceedings. The applicant's purpose was to, on a timely basis, inform users of the time limits which start on the date when decisions are taken or actions occur. For this purpose, the applicant would import data through a web service and periodically update his existing database, which would then be offered to users. The applicant would use the requested data for commercial purposes.

The authority rejected the application as the applicant had requested data which, pursuant to legislation, is available only to eligible persons (the fourth indent of the sixth paragraph of Article 6 of ZDIJZ). In accordance with the provisions of the second and the fifth paragraph of Article 122.a of the Financial Operations, Insolvency Proceedings and Compulsory Dissolution Act the authority only supplies the data, that was requested by the applicant, in a computerised form to a list of eligible recipients. The sixth paragraph of Article 122.a of ZFPPIPP mentions the purposes for which data on insolvency proceedings, supplied in a computerised form to eligible recipients, can be used. The existing regulations do not include the re-use of information as one of the legally allowed purposes for the use of insolvency proceedings data. The authority concluded that the applicant does not affirm that he is a person or institution referred to in the second or the fifth paragraph of Article 122.a of ZFPPIPP nor does he indicate that this data would be used for one of the purposes

specified in the sixth paragraph of Article 122.a of ZFPPIPP.

In the appeal proceedings, the Information Commissioner determined that Article 122.a of ZFPPIPP cannot be interpreted in a way that suggests there are only exclusive recipients. To speak of exclusive recipients would be possible if the data to which they would be entitled were not freely accessible. In the present case, such an explanation is illogical and contradicts the purpose of the act. Consequently, the conditions from point four of the sixth paragraph of Article 6 of ZDIJZ, which is limited to data available only to eligible recipients, are not met, while in the present case, we are clearly dealing with data which must be and are, on the basis of the law, available to everybody. The purpose of the provision of ZFPPIPP in specifying web pages to be used for publication of insolvency proceedings is clear – broad public access which is identical to the applicant's purpose. The goal of re-use of public information is that every applicant has the right to acquire the right to re-use information for commercial or non-commercial purposes under the same conditions as other persons (the fourth paragraph of Article 5 of ZDIJZ). The authority cannot discriminate against applicants within the same or similar category of information re-use. The latter is also specified in Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information which the Slovenian legislator implemented with ZDIJZ. Article 10 of Directive 2003/98/EC regulates the principle of non-discrimination specifying that conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use, as is the situation in the present case. Directive 2003/98/EC and consequently ZDIJZ, foresee the possibility that an authority can grant exclusive rights to re-use information under specific conditions, which according to the Commissioner, could be a reason for refusal of the right to re-use information. But according to the information held by the Commissioner, who is responsible for keeping a record of all the exclusive rights granted, an exclusive right was not granted in this case. The Information Commissioner pointed out that the authority cannot make reference to the fourth indent of the sixth paragraph of Article 6 of ZDIJZ in the case where it finds that all data which is the subject of the application for re-use, is freely available and published on the Internet. In such cases, the responsible authority must specify conditions for re-use of public information which will not discriminate among applicants. The responsible authority must consider all of the above in its reconsideration of the applicant's request.

3.3. General Assessment and Recommendations in the field of Access to Public Information

The Information Commissioner can fairly assess work in the field of access to public information as positive in 2013. Both applicants and responsible authorities are more familiar with the institution of access to public information. The number of complaints received against refusals of access to information in 2013 is comparable to the number from 2012, and there is again an increase in the number of complaints due to the non-responsiveness of first-instance authorities (in 2012 there were 242 such complaints, in 2013 there were 339). Last year the Commissioner also received a large number of questions, initiatives and requests for clarification in connection with the use of ZDIJZ in practice (622).

On the basis of the information stated above and the complaint procedures handled, the Information Commissioner assesses that public awareness of the right to access public information has increased, and most first-instance authorities operated better than the year before. This was also reflected in the percentage of rejection decisions issued by the Information Commissioner, which was higher than in the previous year (44.6%), which means that first-instance authorities ruled correctly more often, and that applicants' complaints were therefore unfounded. The Information Commissioner nonetheless in practice noticed a difference in operations between state authorities and other responsible entities (the broader public sector, bearers of public authority, and public service operators). The latter are still poorly informed about the procedure for handling submitted requests (forwarding the requested information within 20 working days, or issuing a rejection decision), which is seen in the number of complaints against the unresponsiveness of first-instance authorities. It is important to note that in the majority of cases, after prompting by the Information Commissioner on the basis of paragraph 3 of Article 255 of ZUP, matters are resolved in

favour of the applicants, and the responsible authorities forward the requested information. The aforementioned shows that the reason for the unresponsiveness is not a desire to deny access to the requested information, but ignorance of the law, and consequently the incorrect procedural handling of submitted requests.

It is interesting that most of the decisions issued by the Information Commissioner were related to the question of whether the requested document exists (in past years the most common exemption was the protection of personal information), which shows that even in the event of a presumed lack of a document's existence applicants want the Information Commissioner to check the actual status and determine whether or not such information in fact does not exist. It should also be noted that the responsible authorities in the first-instance and the Information Commissioner as the appellate body, are faced with and must deal with increasingly complex cases. Again in 2013, the most complex matters were connected with the access to documentation from public procurement procedures. These procedures require decisions on a vast scope of documentation, the inclusion of third-party participants and the consideration of multiple exemptions in respect of the use of public funds (trade secrets, personal data). The Information Commissioner finds that appeal proceedings are often the result of procedural errors made by the first-instance authority (by the non-inclusion of third-party participants, delayed responses to requests) and unfamiliarity with the legal provisions and implementation of the law in practice, which could be resolved through the regular and mandatory training of officers, dealing with access to public information, from the responsible authorities. Once again in 2013 there were an increased number of complaints against the fees charged for access to public information. As it has for several years now the Information Commissioner, warns about the unacceptable practice of some responsible authorities, charging fees for simply viewing a document (this is free of charge under the Act), and the fact that they wish to "transfer" all their operating costs in this area to applicants.

2013 was also marked by the preparation of amendments to ZDIJZ, intended to widen the scope of responsible authorities, specifically to include all legal entities in which the state, local community, or other public sector legal entity holds a dominant influence. The Information Commissioner warmly welcomes this change, as it has often alerted to the fact in recent years, that these entities include such entities whose operations are directly or indirectly in the public interest, while the public, on the basis of current legislation (ZDIJZ), does not have access to any information about their operations because they are subjects of private law.

In terms of the re-use of public information, 2013 was marked by an amendment to the Directive of the European Parliament and Council of 17 February 2003 on the re-use of public information. The purpose of the proposed amendments to this directive (which was implemented into Slovenian acquis with ZDIJZ) is to ensure an optimal legal framework and a change in public sector culture, to foster the digital content market for products and services that are based on public sector information and to prevent distortions to competition in the market. The proposed amendments should thus contribute to economic growth and the creation of new jobs.

In 2013 the Information Commissioner received six complaints in the area of the re-use of public information, which is more than in the previous year (in 2012, there were two complaints). Once again this year the Information Commissioner collaborated in an international consortium on the LAPSI project (Legal Aspects of Public Sector Information), whose purpose is to establish a thematic network in the field of the re-use of public information. In conjunction with this it was also a co-organiser of a successful International conference which took place in Ljubljana on 24 October 2012 (http://www.lapsi-project.eu/lapsi-20-conferences).

4 ACTIVITIES IN THE FIELD OF PERSONAL DATA PROTECTION

4.1. Activities in the field of Personal Data Protection in the Republic of Slovenia

In the Republic of Slovenia the concept of personal data protection is based on the provisions determined by Article 38 of the Constitution, in accordance with which personal data protection is one of the constitutionally guaranteed human rights and fundamental freedoms in the country. This provision guarantees the protection of personal data, forbids the use of personal data in ways contradictory to the purpose of their collection, ensures everyone the right to be informed about the personal data which has been collected about them, and also ensures the right to judicial protection in the event of their abuse.

For normative regulation of data protection, paragraph 2 of Article 38 of the Constitution is particularly important, wherein it is determined that collecting, processing, purpose of usage, monitoring and protection of the confidentiality of personal data is to be regulated by legislation (general, organic and sector-specific laws). This is a so-called processing model with certain rules for regulating permissible processing of personal data at the legislative level. According to this model, in the area of processing personal data everything is forbidden, except for that which the legislation (in the private sector also individuals' personal consent) expressly allows. All processing of personal data therefore represents an encroachment on a constitutionally protected human right. Such encroachment is thus only permissible if it is expressly determined in the law, which stipulates which personal data may be processed and the purpose of their processing. Appropriate protection of personal data must also be provided. The purpose of processing personal data must be constitutionally permissible, and only data which are appropriate and vital for realising said purpose, may be processed.

Regulating the protection of personal data in an organic act is necessary so as to enable the uniform determination of principles, rules, and obligations, as well as to fill lacunae in the law, which could arise in sectoral laws. Furthermore it is not necessary, that sectoral laws always contain, for example, definitions, regulations regarding the protection of personal data, database catalogues for personal data and the registration of databases, the individual's rights to be informed about data pertaining to them, and questions regarding supervision and the competences of a supervisory body. The purpose of organic law is not to define in detail the ways in which personal data in individual areas can be processed, but above all to define in a uniform manner general rights, obligations, principles, and measures by means of which unconstitutional, illegal, and unjustified encroachments into the privacy and dignity of the individual in relation to the processing of personal data are prevented. Therefore, sectoral laws must clearly determine which databases of personal data will be established and maintained in individual areas, the types of personal data that individual databases will contain, the manner in which personal data will be collected, the possible limitations of the rights of the individual, and above all, the purpose of processing the collected personal data. In terms of individual protection, it is highly recommended that in sectoral law a statutory time limit for the storage and retention of personal data is also determined.

The Personal Data Protection Act , which the National Assembly of the Republic of Slovenia adopted on 15 July 2004, came into force on 1 January 2005 and was supplemented in July 2007. It was necessary, above all, to adopt this Act due to the accession of the Republic of Slovenia to the European Union and due to the obligations arising therefrom, for harmonising personal data protection with the provisions of Directive 95/46/EC of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and the free flow of such data.

ZVOP-1 is not just an organic act, but in part IV it is also a so-called sectoral law which by means of an exact definition of rights, obligations, principles and measures, provides data controllers with a direct legal basis for personal data processing in the areas of direct marketing, video surveillance, biometrics, recording the times of persons entering and exiting premises, transfer of personal data to third countries, as well as professional monitoring.

In addition to the Constitution, ZVOP-1, ZIngP, and acts which in detail regulate the processing of personal data in a given area, in the Republic of Slovenia the provisions of

the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was ratified and published in 1994 are used.

Due to suspicion of violations of the provisions of ZVOP-1, in 2013 the Information Commissioner conducted 712 inspections, of which 253 pertained to the public sector and 459 to the private sector. On the basis of complaints against public sector legal entities, it initiated 231 inspection procedures, and an additional 22 procedures were initiated ex officio, e.g., if, on the basis of reports in the media it suspected a violation of personal data protection or if such a suspicion arose during planned audits. On the basis of complaints associated with the private sector it initiated 435 inspection procedures and initiated 24 procedures ex officio. The number of complaints and appeals due to the suspicion of violations of ZVOP-1 increased slightly in comparison to the statistical data for 2012 (747 in 2012 vs. 852 in 2013), although the total number of inspection procedures was slightly lower than in 2012 (when there were 725). The number of complaints that the Information Commissioner received was slightly higher than the number of open inspection procedures or initiated inspection procedures, as it received several complaints against the same responsible entity. Thus in 2013 the Information Commissioner received 241 complaints against responsible public sector authorities (in 2012 there were 237 complaints), and 611 complaints against responsible entities in the private sector (in 2012 there were 510). The higher number of complaints against individual responsible entities is more obvious in the private sector, especially against those who carry out direct marketing and send their offers to a large number of people.

The Information Commissioner dealt with cases relating to the following presumed violations of ZVOP-1:

- unlawful disclosure of personal data: the transfer of personal data to unauthorised users by data controllers and the unlawful publication of personal data, e.g. on the Internet or in other media (68 cases)
- unlawfully collecting or requiring personal data (43 cases)
- cookies (28 cases)
- inadequate security of personal data (26 cases)
- unlawful video surveillance and inappropriate use of video footage (15 cases)
- direct marketing (7 cases)
- other: contractual processing of personal data, illegal destruction of personal data, processing of inaccurate and expired personal data, personal data processing in a manner in contradiction with the purpose of collection, refusals to supply personal data, as part of ex officio inspection procedures the Information Commissioner verified a total of 66 cases regarding the full implementation of the provisions of ZVOP-1.

Complaints were filed and procedures ex officio were initiated against the following groups of responsible authorities in the public sector:

- public funds, institutions, agencies and other public authorities (118 cases), of which 42 were against educational institutions and 20 against health institutions,
- state authorities (108 cases), of which the courts, prosecutor's office, and Attorney General accounted for 19 cases,
- municipalities (27 cases).

Figure 4: The number of cases dealt with due to suspected violations of the provisions of ZVOP-1 between 2006 and 2013.

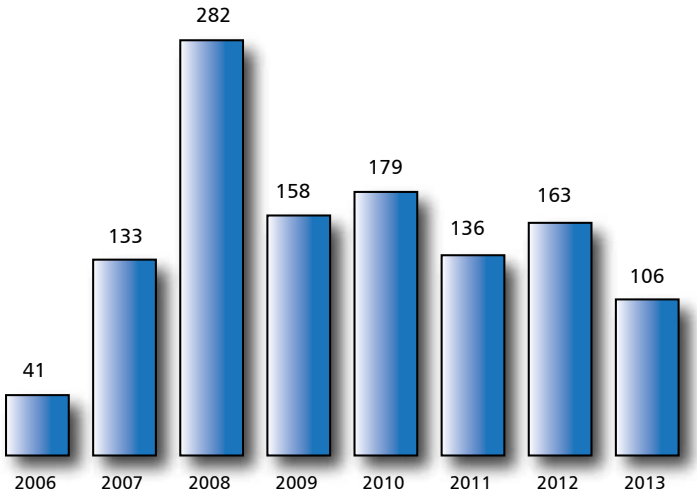
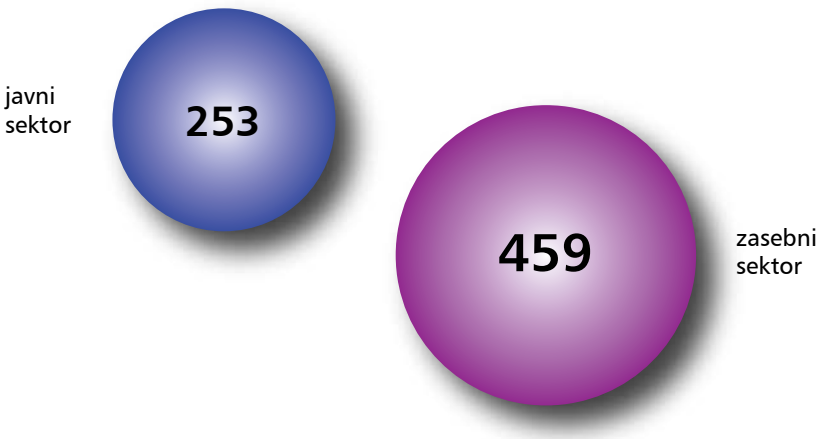


Figure 5: Suspected illegal processing of personal data in 2013, a comparison between the public and the private sectors.



Due to violations of the provisions of ZVOP-1 in 2013, 106 offence procedures were initiated, of which 18 were against legal entities in the public sector and their responsible persons, 62 against private sector legal entities and their responsible persons, and 26 against individuals (this number also includes responsible persons from state authorities and self-governing local communities, as in accordance with ZP-1, the Republic of Slovenia and self-governing local communities are not held accountable, but their responsible person is). If a violation is determined, the minor offence authority can, in accordance with Article 53, issue a warning if it deems that the violation committed is not serious and if the authorised official deems that, given the significance of the action, a warning is a sufficient measure. If a more serious violation has been committed, the minor offence authority issues a decision on the violation, imposing a sanction on the offender. In accordance with Article 4 of ZP-1, the sanctions for a violation are a fine and a warning, and according to Article 57 of ZP-1 fines can be paid via a fixed penalty notice i.e. payment order.

In minor offence proceedings, including proceedings finalised from previous years, in 2013 the Information Commissioner issued:

- 26 warnings
- 72 decisions on a violation (36 warnings and 36 fines)
- The number of decisions issued on violations was lower than in 2012 (there were 119 in 2012), but there were more warnings issued (there were 17 in 2012).

In accordance with principles of economy within the framework of inspection procedures, the Information Commissioner issued 90 warnings for minor violations on the basis of Article 53 of ZP-1 (87 in 2012, 75 in 2011), 25 (24 in 2012) in the public and 65 (63 in 2012) in the private sector.

Offenders submitted 12 requests for judicial protection against decisions issued (against 16.7% of decisions issued vs. 25.2% in 2012), of which 11 were against fines and the other against a warning. The relatively small number of submitted requests for judicial protection indicates that offenders realise the gravity of the offences they have committed. Almost all of the requests for judicial protection were submitted against fines issued, which is a result of the fact that fines under ZVOP-1 are very high, especially for a combination of offences. The Information Commissioner does not have the power to decide on the amount of the fine imposed (in expedited offence proceedings, it can impose a fine upon the offender in the amount that is prescribed, if it is prescribed within a range, then the lowest prescribed amount is imposed). Only the court has the power to reduce an offender's sanction below the prescribed threshold if the Act allows for this, or if it finds that there were special extenuating circumstances which would justify the imposition of a lesser sanction. The Information Commissioner imposes a fine when there is a violation in which the personal data protection rights of an individual were seriously encroached upon, or in cases of the abuse of personal data by authorised persons of a given controller who attained access to personal data in a certain database for the purposes of performing their job.

In 2013, the Information Commissioner stayed nine offence proceedings on the basis of insufficient evidence for measures according to ZP-1, or because it was found that the action alleged was not in fact a violation.

In 2013, the Information Commissioner received 24 judgements (rulings or decisions), in which local courts ruled on submitted requests for judicial protection against decisions on violations which the Information Commissioner had issued in previous years:

- the request for judicial protection was rejected as unfounded and the Information Commissioner's decision upheld (10 cases),
- the request for judicial protection was upheld, the Information Commissioner's decision overruled, and the offence proceedings halted (7 cases),
- the request for judicial protection was upheld in the part pertaining to the sanction imposed, with the result that the offender's sanction was changed or the amount of the fine was reduced, but the request for judicial protection was rejected as unfounded (6 cases),
- the request for judicial protection was upheld in such a manner that the legal classification of the violation in the contested judgement was amended (1 case).

In three cases where the local court stayed the offence proceedings, the Information Commissioner appealed against the court's ruling in a higher court. In 2013 the High

Court decided on one case, in which it upheld the Information Commissioner's appeal, overturned the local court's ruling, and returned the case for reconsideration.

In 2013, the Information Commissioner received 2,460 requests for a written clarification or opinion in connection with specific questions. The number of requests has continued to rise slightly over the past several years: In 2012, there were 2,191 requests, and 2,143 in 2011. Requests for opinions and clarifications are more complicated, which can be attributed to the fact that the public is ever more familiar with ZVOP-1 and with the rights of the individual that arise from it. For more complex questions and questions to which it had not yet responded, the Information Commissioner issued 71 opinions and clarifications, while to individuals posing questions which had previously been answered, simply a brief response was sent, referring them to an already issued opinion. There were 2,389 such brief responses and referrals. A large portion of the opinions are published at https://www.ip-rs.si. The Information Commissioner also gave verbal opinions and explanations. A state supervisory officer is on call everyday and is available to answer questions over the phone.

In 2013, the Information Commissioner received 11 requests for permission for the implementation of biometric measures. Eleven decisions were issued, wherein the Commissioner considered and decided on the permissibility of the implementation of biometric measures. Of these, five were issued in proceedings which had begun in 2012. In four cases, the Information Commissioner fully approved requests for the implementation of biometric measures, four cases were partially approved, and three requests were denied.

The Information Commissioner fully approved a request from an applicant who, for the purposes of protecting people and property, wanted authorised employees when entering the vicinity of the applicant's reactor to gain entry by using three fingerprint scanners. It also fully approved a request from an applicant that, for the purpose of protection of trade secrets, wanted permission to implement biometric measures based on face-recognition for authorised employees to be granted entry to the applicant's IT security room. The Information Commissioner also approved a request from an applicant who, for the purposes of protecting trade secrets wanted permission to implement biometric measures based on fingerprint recognition, specifically for entry to two offices of the President of the applicant's Management Board, two offices of a Management Board Member, and the office of the applicant's head secretary. An applicant wanted to use biometric measures to monitor access to some of the offices of the company's management where documentation containing trade secrets is kept, and also stated that apart from trade secrets, other protected resources included the carrying on of the business, the security of property, and the protection of confidential data in accordance with ZBan-1 (the Banking Act). The Information Commissioner also approved a request from an applicant who, for the purposes of security of property and protection of trade secrets wanted permission to implement biometric measures based on fingerprint recognition for those of the applicant's employees who have access to the area where precious metals are kept, and to the safe. In the proceedings the applicant proved that monitoring access to rooms where precious metals are stored and processed is absolutely necessary from the point of view of protecting property.

The Information Commissioner partly approved four requests for the implementation of biometric measures; in three of the procedures it partially approved the requests for three connected companies which have offices in the same building, and the requests which referred to implementing logically identical biometric measures. In relation to the connectedness of the three companies, the Information Commissioner emphasised that, despite such a connection, each of them individually controlled personal data which would be processed in implementing said biometric measures, and that each of them would need to manage, independently of the other two companies, a separate database of personal data, such that each would administer their own database of personal data arising from the implementation of biometric measures for their own employees, and it would not have access to the personal data from the databases of the other two connected companies, nor could it process such data. The Information Commissioner allowed individual applicants to implement biometric measures using fingerprint scanners for numerous purposes:

- for the purpose of protecting people and property, for control over entry to the applicant's warehouse facilities where medical materials and equipment are stored, specifically for the employees who are authorised to enter these facilities;
- for the purpose of protecting trade secrets, for control over entry to the Director's

office which is located at the applicant's headquarters, specifically for the Director and his secretarial staff;
- for the purpose of protecting trade secrets, for control over entry to two areas where documentation is stored relating to public procurement procedures, specifically for employees who are authorised to enter these areas;
- for the purpose of protecting property and trade secrets, for control over entry to a server room, specifically for the system administrator of the applicant, who is authorised to enter the server room.

The Information Commissioner rejected one applicant's request for the implementation of biometric measures:
- for entry to the applicant's offices, through the building's main entrance and for entry into the foyer which leads directly into the applicant's work areas; the applicant wanted to implement biometric measures for all employees.
- For entry into two conference rooms located in the applicant's offices; the applicant wanted to implement biometric measures for the Director and secretarial employees. The Information Commissioner allowed an applicant to implement biometric measures for the protection of people and property, specifically for the use of fingerprint scanners for those employees who perform their work in the stated areas and who have authorisation to access such areas: for entry into rooms within a dialysis centre, where the applicant mixes and stores dialysis solution, for entry into rooms within the dialysis centre where the applicant stores medicine, for entry into rooms within the dialysis centre where the applicant keeps its patients' medical records. The Information Commissioner rejected the applicant's request for implementing biometric measures at the main entrance to its dialysis centre for employees entering the centre and for the registration of their time in the workplace.

The Information Commissioner entirely rejected three requests for the implementation of biometric measures, in the case of the request by an applicant to implement biometric measures for all employees entering their workplace through the main entrance; the request of an applicant who wanted to implement biometric measures for keeping a time log of its employees; and the request of an applicant who wanted to implement biometric measures for all employees and students entering the workplace through the main entrance.

In 2013, the Information Commissioner received 14 requests for transfers of personal data to third countries, one applicant withdrew their application. The Information Commissioner issued 16 decisions, five of which had been cases received for resolution in 2012. All applicants were allowed the transfer of personal data outside the Republic of Slovenia, specifically: a company which markets medicine was allowed to transfer and forward to its contractual data processors in the USA, India and New Zealand, personal data on employees, part-time workers and consultants in order to facilitate e-mail and reporting services in MS Exchange; a trading and investment firm was allowed to transfer and forward to its contractual data processors in other countries (namely India, the Philippines, the USA, China, and Costa Rica) personal data on its employees, contractual workers and consultants, existing and potential customers and sales agents, whose personal data are processed in order to support procurement, to assist with fulfilling obligations to suppliers, supporting operations and financial and accounting data processing; two Slovenian subsidiaries of foreign distribution firms were allowed, to transfer and forward personal data pertaining to past, current, and future employees, volunteers, colleagues and partners, past, current, and future customers, past, current, and potential consultants, experts, suppliers, contractors, subcontractors, representatives and intermediaries, claimants, correspondents, visitors and inquirers, beneficiaries, dependants, parents, caregivers and contact persons in cases of emergency, to their contractual data processors in the USA, Panama, Malaysia, and India for the purposes of providing certain IT products and services;, an energy measurement and management company was allowed to transfer and forward to its contractual data processor in the USA, personal data pertaining to representatives and end users, including workers, co-workers, and customers of the data transferrer; as well as of individuals who are attempting to give or to transfer personal data to users of services which the data importer provides for the purpose of completing tasks related to the provision of Microsoft cloud computing services; a petroleum company was allowed to transfer and forward to its contractual data processor in Vietnam, personal data of natural persons included in its loyalty program, for the purposes of transferring data from paper to a digital format; a bank was allowed to transfer and forward to its contractual data processor in the Russian

Federation, personal data of bank customers, bank employees and contractual partners, for the purposes of IT support.

In assessing the legal basis for the intended forwarding of personal data, the Information Commission found that in all the cases stated the personal data was to be forwarded to contractual processors (data importers), who were to process personal data in the name of and on behalf of the data controllers (transferrers).

In the following three cases, the data would be sent according to binding corporate rules. After reviewing the documentation submitted by the data transferrers, the Information Commissioner found that they are obligated to follow binding corporate rules which were adopted by the multinational group which they are a member of. The procedure for adopting binding corporate rules includes a procedure before a Lead Authority for personal data protection with regard to the headquarters of the appropriate member in the EU (in the cases at hand these are Denmark and France), which confirms the binding rules and thus ensures that they meet legislative requirements for personal data protection in the EU, as well as a mutual recognition procedure, in which other authorities from relevant EU member states are also included. The Information Commissioner also cooperated in a mutual recognition procedure for binding corporate rules.
On the basis of binding corporate rules, the Information Commissioner: allowed a pharmaceutical company to transfer and forward, to its contractual data processor and other administrators or other group members, a portion of which are from third countries, personal data of employees and co-workers, suppliers and business partners, participants in clinical studies and researchers, users and customers, as well as medical workers, for the purposes of: administration, reporting, organization, employee management, communication, maintaining business operations, coordination, evaluations of health effects, patient support, sales and marketing, completing financial and other transactions, and performing pharmacological vigilance; allowed an auditing and other financial accounting services firm to transfer and forward to other companies in its business group: employee data for the purpose of staff management, data on customers for the provision of expert services and operations, and other business data for the purposes of supply and procurement of goods and for providing services to companies, for the purpose of financial and other aspects of managing operations (recipients of the data include companies in the group, employers, education institutions, customers, financial organizations, associations, the police, regulatory bodies, etc.); allowed a company which markets pharmaceutical products to transfer and forward to its contractual data processor and other personal data controllers in third countries, being members of the group to which the transferrer belongs, personal data of employees, customers, suppliers, and third parties with whom the transferrer works for the purpose of the group members' regular operations.

In 2013, the Information Commissioner received six requests for the linking of personal data databases. It issued five decisions, allowing three controllers (The Supreme Court of the Republic of Slovenia received two decisions) to link personal data databases, and in one instance did not allow linking. The Information Commissioner allowed the Ministry of the Interior and Public Administration to link the Register of Licences and Register of holders of Service Cards, which it keeps in accordance with the Private Security Act , with each other and with: the Slovenian Central Population Register, Slovenian Business Register, and the Register of insured persons with compulsory health insurance. It allowed the Ministry of Agriculture and the Ministry of the Interior a direct computer link to the Register of Subjects (Innovative Environment) and the Central Population Register It allowed the Supreme Court of the Republic of Slovenia to link the Information system on Civil Claims with: The Central Population Register, the Central register of book entry securities, Register of insured persons with compulsory health insurance, the Register of transaction bank accounts, and the eINS Information System (insolvency register).

The Information Commissioner rejected the request from the Ministry of Education, Science and Sport for linking the Central register of the participants in education and schooling (CEUVIZ) to the Register of persons entitled to State Budget Funds for co-financing parents' financial contributions for Kindergartens (SPS).

In 2013, the Information Commissioner initiated 68 complaint procedures regarding the right of familiarisation with and access to one's own personal data (63 procedures in 2012, 85 in 2010 and 2011). Within the framework of complaint procedures, the Information

Commissioner also resolved complaints where individuals were unable to acquire medical documentation in accordance with ZPacP. There were 11 such cases in 2013, (4 in 2010, 18 in 2011, 10 in 2012). After examining the complaints, the Information Commissioner found that in comparison to previous years the percentage of data controllers' lack of responsiveness, i.e. cases in which data controllers failed to respond to individuals' requests for access to their own personal data, remained at the same level (52%). In the event of a data controller's lack of responsiveness, as well as in cases where access is denied, individuals can file a complaint with the Information Commissioner.

In 2013, the Information Commissioner filed two requests for a constitutional review of the legislation. The Information Commissioner filed a request for a constitutional review of paragraphs 1, 7, and 8 of Article 20 of the Tax Procedure Act (publication of tax defaulters' personal data), as in the course of an inspection procedure it determined that, with the use of the contested legislative provisions, an individual's right to personal data protection as prescribed by Article 38 of the Constitution of the Republic of Slovenia, is violated. The Information Commissioner also filed a request for a constitutionality and legality review of Chapter XIII (data storage), Articles 162–169 of the Electronic Communications Act, as in an inspection procedure it found that a database that the responsible entity compulsorily saves and stores, increases each day with the inclusion of millions of new entries. The data which operators must keep for 14 or 8 months following contested provisions of ZEKom-1 are data on traffic and location and other related data, which identify the subscriber or user of a public communication service. It is the Information Commissioner's opinion that this measure is not appropriate for achieving the goals, namely: better research of (serious) crimes, the security and defence of the country.

In relation to the request for a constitutional review of the Police Act, which it filed with the Supreme Court of the Republic of Slovenia, the Information Commissioner submitted its opinion, believing that the Constitutional Court would find its explanations useful in helping it to reach a decisions on the constitutionality of the contested provisions covering the storage of DNA samples in police records. During the court's decision making process a new act, the Police Tasks and Powers Act was approved, which somewhat changed the regulations for the processing of personal data in DNA investigation records. After reviewing the new arrangements (Articles 128 and 129), the Information Commissioner found that they still violated the principle of personal data protection regarding the prohibition of excessive measures by the state (principle of proportionality), as there is no differentiation between convicted and innocent individuals, with the same storage retention periods for both groups. If an individual has been charged and had an oral swab taken, and a DNA profile determined, and later the prosecutor dismisses the complaint, it does not result in erasure of this individual from this database. Even with the new measures, the only reason for erasure from the DNA registry is still the expiry of extremely long retention periods, which are the same for both convicted as well as exonerated individuals.

In 2013, the Constitutional Court ruled on the request for a constitutional review of the provisions of Article 29 of the Prevention of Restriction of Competition Act (ZPOmK), which the Information Commissioner filed in 2012. At the time the Commissioner raised the question of the acceptability of the behaviour of supervisory authorities, who, by exercising their powers within the scope of administrative-inspectional and/or minor offence proceedings, and referring to the legal basis of the provisions, however without a court order, and for purposes other than those defined in Article 37 of the Constitution of the Republic of Slovenia, infringe upon (electronic) communication. The Constitutional Court rejected the Information Commissioner's request due to the lack of procedural requirements (Decision No. U-I-92/12-13) and decided that the Information Commissioner may not conduct inspection monitoring on the implementation of ZVOP-1 in such a way that in executing its legally provided powers it interferes with individual legal proceedings conducted by competent state authorities. The Information Commissioner accepts the Constitutional Court's decision regarding competency, but regrets that the court did not make a substantive judgement (it could also have issued a warning on the limitation of competency in this case), as it is of the opinion that the problems raised in the request are serious and that all supervisory authorities would benefit from the court taking a stance on these problems.

4.2. Selected Cases of violations of Personal Data Protection

Recording of telephone conversations by a public institution

The Information Commissioner initiated an inspection procedure against a public institution after establishing that as the responsible authority it had installed an automated information system for calls to its contact centre phone number, which prior to allowing callers to talk to a contact centre officer, informed them that to ensure quality of service their conversation would be recorded.

The inspection procedure established that the responsible authority had introduced the recording of telephone calls with a view to maintain and improve quality of service. The audio recordings of the telephone conversations were used to prepare proposals for a training program for call centre operators (rhetoric training, dealing with clients in difficult situations, etc.). Based on the most frequently asked questions during telephone conversations the authority was also able to establish what additional information should be made available to the public to ensure individuals enjoy the highest level of access possible. In its explanation, the responsible authority stated that even though it had no explicit legal basis for recording telephone conversations, in its opinion, if the caller is appropriately informed, conversations could be recorded on the basis of the provisions of ZEKom-1.

During the inspection procedure the Information Commissioner first established that in accordance with the definition of personal data under point 1 of Article 6 of ZVOP-1, a person's voice or speech also represents personal data relating to an individual, and that the audio recording of an individual's voice or speech together with other information that make the individual identifiable, undoubtedly represents a database of personal data. As is the case with other personal data, audio recordings of an individual's voice or speech, which make an individual identifiable, must also have an appropriate legal basis for their processing. The responsible authority, as a public sector legal entity, can only process personal data in this particular case if the processing of personal data is provided for by statute (paragraph 1 of Article 9 of ZVOP-1). Personal data may in exceptions be processed where they are essential for the exercise of lawful competences, duties or obligations of the public sector, provided that such processing does not encroach upon the justifiable interests of the individual to whom the personal data relate (paragraph 4 of Article 9 of ZVOP-1).

A public sector responsible authority could therefore record telephone conversations based on the legal provisions in the sectoral act governing the confidentiality of electronic communications (ZEKom-1) or on the basis of an exception referred to in paragraph 4 of Article 9 of ZVOP-1. On the basis of the provisions of paragraph 5 of Article 147 of ZEKom-1, all forms of surveillance or interception of communications (such as listening, recording, retention of communications) by third parties, without the consent of the users concerned is prohibited, except in those cases exhaustively listed. In accordance with the provisions of paragraph 7 of Article 147 of ZEKom-1, recording is permitted in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication, on condition that the customer or client in the communication is notified in advance of the recording, its purpose and the period of its retention. The recorded communication must be erased as soon as possible and, in any case, no later than by the end of the period during which the transaction can be lawfully challenged.

The Information Commissioner concluded the procedure, establishing that despite giving prior notice of recording, the responsible authority had no legal basis for these particular recordings. The provisions of paragraph 7 of Article 147 of ZEKom-1 only permit recording of communications "for the purpose of providing evidence of a commercial transaction or of any other business communication". In this context, the term "business communication" must be strictly interpreted. It must be taken into account that paragraph 7 of Article 147 of ZEKom-1 provides an exception to the general prohibition under paragraph 5 of that Article, which means that recording on the basis thereof is only permitted in exceptional, duly justified cases. In addition, according to the retention period of the recorded communication, which paragraph 7 of Article 147 of ZEKom-1 defines as "no later than

by the end of the period during which the transaction can be lawfully challenged," it is clearly evident that only "business communication" leading to the conclusion, change or termination of a particular business relationship can be recorded. In accordance with the above, even if callers were informed of the recording, its purpose and the duration of the retention period, the responsible authority could only record telephone conversations that it needed in order to ensure commercial transactions, or any other conversations that may lead to the conclusion/change/termination of a particular business relationship. According to the Information Commissioner, the purpose of "maintaining quality of service" cannot be regarded as a legitimate purposes for which ZEKom-1 allows the recording of conversations in exceptional cases.

Furthermore, the authority did not demonstrate that telephone conversations were recorded on the basis of the provisions of paragraph 4 of Article 9 of ZVOP-1, which provides an exception to the general requirement of a necessary legal basis for the processing of personal data in the public sector.

Therefore, the Information Commissioner ordered the authority to stop recording telephone conversations at its call centre phone number, to destroy stored recordings and also to stop using the automated information system notification "To ensure quality of service your call is being recorded".

Inadequate security of sensitive personal data by a health care institution

The Information Commissioner carried out an inspection visit at a health care institution, the purpose of which was to verify the adequacy of procedures and measures to protect personal data, and to verify the observance of the Commissioner's decision issued to the institution as the responsible authority in 2007, in connection with ensuring the security of personal data during their processing.

During the inspection visit it was found that the authority was using software that allowed traceability of the personal data processing, namely, who accessed the personal data and when it was accessed and what the purpose of the personal data modification or access was. Before the inspection, the responsible authority had not been carrying out any internal controls of the legality of access to personal data. During the inspection the Information Commissioner obtained internal documents regulating to the security of personal data, in respect of which it was found that they did not determine the procedure for obtaining or using audit trails of accesses to personal data. It was also found that user passwords did not expire and that all doctors and nurses had the same access rights. Any doctor can view data on all patients who were or are still being treated at the responsible authority. The responsible authority argued, in this respect, that it was essential that the attending doctor could immediately obtain all patient data needed for their professional work.

Article 24 of ZVOP-1, which regulates the security of personal data, provides, inter alia, that procedures and measures to protect personal data must be adequate in view of the risk posed by processing, and the nature of the specific personal data being processed. Security mechanisms and measures must be adjusted according to the risk posed by the processing of personal data. First, it is therefore necessary to properly assess the risk. The Information Commissioner found that in its database of personal data the responsible authority processed a large amount of personal data, a large proportion of which were, with regard to the authority's field of activity, sensitive personal data, whose misuse could have serious, time-consuming and in some cases irreversible consequences for the individual. Given the sensitivity of the data processed by the responsible authority, any risk analysis should have shown that these are data with a high or perhaps the highest level of risk, and therefore measures and procedures to protect such personal data at the highest level should have been in place to minimise if not negate the risks to which they are exposed.

Internal controls aimed at detecting unlawful processing of personal data and the adoption of procedures and measures to prevent such processing represent measures aimed specifically at the protection of especially sensitive personal data. Such internal controls should be carried out by data controllers who process large amounts of personal data or who process sensitive personal data, and by all other data controllers for which risk analysis shows that such a measure is necessary and appropriate with regard to the high risks involved. Without

this type of control it is virtually impossible to detect unlawful access to personal data in cases of major data controllers and large amounts of data. Since implementation of internal controls of the legality of personal data processing is considered a measure that can also lead to excessive processing of personal data, disproportionate demands on employees and other consequences, it is appropriate that it be, as a measure, accurately defined, and that its scope, frequency, implementers, goals, manner of implementation, reporting, required action and other elements be defined in an appropriate internal document, so enabling a protocol of internal control whose proportionality and effectiveness can thus be ensured.

The Information Commissioner therefore ordered the authority to formalise the protocol for the implementation of internal controls in an internal document, defining its scope, frequency, implementers, goals, manner of implementation, reporting and required action in the case of perceived unlawful processing of personal data.

During the inspection visit the Information Commissioner also noted that the responsible authority, for the purpose of access to the information system which consequently allowed traceability of the personal data processing, was using a system of user names and passwords that did not expire, and that there were no requirements regarding the complexity of the chosen password, thus deviating from accepted good practices in the field of IT security. Considering the nature of the personal data processed by the responsible authority in the information system, and taking into account the risks posed, such practices are unacceptable. Consequently, the Information Commissioner ordered the authority to include password regulation policy in an internal act and to start implementing it for this information system.

Police powers in the case of access to web users' data

The Information Commissioner received a complaint related to the use of police powers in connection with the acquisition of data on users of websites which have content that is submitted by service recipients or users (these are websites such as on-line forums, media websites, etc.). Since the complaint raised suspicions that in an unknown number of cases personal data of users of on-line forums had been obtained without the proper legal basis, the Information Commissioner requested that the police provide clarification on how many times and from which on-line forum operators they had requested users' personal data in 2012 and on what legal basis, as well as an explanation as to why they used the provisions of ZKP instead of the provisions of ZEPT for the acquisition of personal data from on-line forum operators who are information society service providers (and not from operators of electronic communications networks).

Based on the analysis of the data provided by the police, the Information Commissioner noted the following:

- In 2012, the police requested data on on-line forum users from information society service providers 35 times.
- Just like any other user of personal data, in its request for data the police should have indicated as much information as needed for the data controller to be sure of the existence of a legal basis as well as the necessity of the information requested. The police should therefore have, at the very least, indicated the legal qualification of the criminal offence prosecuted ex officio, which the police did not do in 30% of its written requests.
- Most often Article 148 of ZKP, Article 55 of ZPol or paragraph 3 of Article 149.b of ZKP were indicated as the legal basis for requesting personal data.
- Not even in one of its first requests to a service provider, did the police refer to the provisions of Article 8 of ZEPT, which read as follows: Service providers shall provide all competent authorities, at their request, data on the basis of which it is possible to identify the recipients of their service (name and surname, address, company name, e-mail address) within three days of receipt of the request. Service providers shall communicate the above data for the purpose of detection and prevention of criminal offences on the basis of a court order and, in the absence of a court order, if so provided by a sectoral law.
- In view of the information obtained and at the suggestion of the police a court order was issued to information society service providers in four cases.
- In 23 cases (66%), information society service providers provided data on users without

a court order, at the written request of the police, in two cases (6%) data were provided on the basis of a court order, while in seven cases data were not provided (or it is not clear from the documentation obtained whether the data were provided).

- In most cases, the police request data on the IP address of users, i.e. traffic data.
- It is also evident from the findings that in one case, the police requested an information society service provider to withdraw a photograph; in one case, the police requested data on all users of a specific domain for a period of almost three months, and in one case, the police requested the contents of SMS messages, phone numbers of recipients, the number of SMS messages sent and other data.
- The Information Commissioner has not received an answer to the question why the provisions of ZKP were used instead of the provisions of ZEPT for the acquisition of personal data from on-line forum operators who are information society service providers.

Based on the analysis carried out, the Information Commissioner found that the police apparently were not aware of the provisions of ZEPT or were ignoring them, since not even in one of their requests in 2012 did they refer to the applicable provisions of ZEPT. Rather, the police referred inappropriately to provisions of ZKP, ZPol or even ZVOP-1, while in some cases there was no legal basis indicated at all. It is also evident that there is a lack of knowledge of the differences between the operators (providers of publicly available electronic communications networks and services) whose operation is primarily governed by ZEKom, and operators of websites (information society service providers) whose operation is primarily governed by ZEPT. Apparently, not even the information society service providers themselves are aware of the provisions of ZEPT, since in most cases they deliver data to the police without a court order. Considering all of the above, it is not just a question of the legality of personal data processing (such as transmitting and further use of personal data), which is monitored by the Information Commissioner, but also of the applicability of such collected evidence in criminal proceedings. If evidence is obtained in violation of constitutionally protected human rights or in breach of the provisions of ZKP, the court's decision cannot be based on such evidence.

The Information Commissioner informed the Ministry of the Interior and the Office of the State Prosecutor General of the Republic of Slovenia of the findings of the inspection and suggested the preparation of a report in response thereto which would include a list of measures to address the identified deficiencies. By the end of 2013, the Information Commissioner received an interim report from the Ministry of the Interior. The case will continue to be addressed in 2014.

Loss of voters' signatures to a call for a legislative referendum

Following media reports on the missing lists with signatories, gathered by the Chemical, Non-metal and Rubber Industry Trade Union of Slovenia (KNG), calling for a legislative referendum on the Act Defining the Measures of the Republic of Slovenia to Strengthen Bank Stability, the Information Commissioner initiated an ex officio inspection procedure at the National Assembly and the Ministry of the Interior regarding the implementation of the provisions of ZVOP-1.

In the course of the inspection, it was found that upon receipt of the list with personal data of the initiators of the referendum on ZUKSB, delivered personally to the National Assembly by representatives of the KNG Union, the number of signatures was not known, nor was the number of signatures properly verified or documented by the National Assembly upon the acceptance of the list. How many sheets of paper the list of initiators (i.e. signatories) was comprised of was neither verified or documented when being photocopied nor during the handover of the list to the Ministry of the Interior for the authenticity of signatures to be verified. Nor did the Ministry appropriately document and verify the actual size of the list with personal data upon receipt of photocopies from the National Assembly. When an employee at the Ministry distributed the list among 28 employees for verification, the distribution itself was not properly recorded. Also, the responsible person at the Ministry did not record the number of sheets returned following verification of the list. According to both responsible authorities, this was their long-standing practice upon receipt of referendum initiatives. It was only after the intervention of the initiator in response to the apparent insufficient number of signatures, that an internal verification was carried out

at the National Assembly and sheets were counted, establishing that the original list of signatures received was comprised of of 307 sheets of paper; the Ministry of the Interior returned photocopies of 271 sheets that had been verified, thus it was established that 36 photocopied sheets with personal data of 361 signatories were missing.

In the absence of the adequate recording of the number of sheets comprising the list of signatories, both at the National Assembly (upon direct delivery, when photocopying, on return from the Ministry of the Interior) and at the Ministry of the Interior (upon receipt from the National Assembly, upon distribution for verification to officials at the Ministry), the Information Commissioner subsequently could not establish which sheets of the list with personal data had been processed at a particular point, but it was nevertheless established that both responsible authorities had acted contrary to the requirements of ZVOP-1 with respect to the protection of personal data, as with the failure to verify and record the size and content of the list of signatories to the voters' initiative calling for a legislative referendum, which represents a database of sensitive personal data, they had not provided procedures and measures to protect personal data laid down in Article 24 of ZVOP-1, with which personal data is protected and which prevent accidental or deliberate unauthorised destruction, modification or loss of personal data (so-called internal traceability). As personal data controllers both responsible authorities were obliged to provide adequate protection and integrity of the entire list of signatories during the entire course of its processing.

In addition, for both responsible authorities conduct in contravention of paragraph 3 of Article 22 of ZVOP-1 was identified, as they did not provide so-called external traceability. Neither the National Assembly upon delivery of the list to the Ministry of the Interior for verification, nor the Ministry of Interior upon returning the verified list back to the National Assembly ensured that it would be possible to subsequently establish what personal data of signatories of the initiative had or had not been delivered to the other responsible authority.

Due to the irregularities identified, the Information Commissioner imposed a sanction against the responsible persons at the National Assembly and at the Ministry of the Interior in accordance with ZP-1.

Premature destruction of medical records

On the basis of a complaint, the Information Commissioner initiated an inspection procedure against a responsible entity (health spa) because of a claimed unlawful destruction of an individual's medical records just three years after their treatment was completed.

During the inspection it was established that the internal acts of the responsible entity set different retention periods for personal data of health service users (15 or 5 years) and that, as a general rule, the old medical records were extracted and destroyed once a year. Despite these retention periods the responsible entity, due to limited space and limited technical possibilities for storage of very large quantities of medical records in paper format, only kept medical records for three years after the completion of the health spa treatment. The responsible entity reviewed medical records annually and prepared them for destruction. The medical records intended for destruction were weighed, but no list of patients' names, whose records were destroyed, was produced due to the very large number of cases (approx. 2,500–3,000). During the inspection it was also established that data in electronic form to be transmitted to the Health Insurance Institute of Slovenia (ZZZS) for the purposes of payment of the services provided and discharge letters, were stored by the responsible entity for a longer period of time.

In accordance with point 3 of Article 6 of ZVOP-1, storage of personal data is also considered a type of processing of personal data, for which it is necessary to have a proper legal basis. Rules relating to personal data retention periods are set out in Article 21 of ZVOP-1, which in paragraph 1 provides that personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed. On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless pursuant to the legislation governing archival materials and archives they are defined as archival material, or if for an individual type of personal data

the legislation does not provide otherwise.

It is clear from Article 13 of the Health Services Act that health spas provide specialist outpatient services, which represent a continuation or supplement of basic health care services and comprises an in-depth diagnosis, treatment of illnesses or medical conditions and provision of outpatient rehabilitation. Article 19 of ZZDej further provides that the health spa medical services cover preventive care and specialist outpatient and inpatient rehabilitation, including the use of natural healing resources. This activity is carried out by natural health spas, if they meet the conditions laid down by the Minister responsible for health. In view of the above, health spas are considered health care providers, so they must comply with the provisions of a special law, i.e. ZZPPZ, regarding the storage of personal data. Further to the Annex to ZZPPZ, under point no. IVZ 1, it is determined that the patient record and clinical history are to be stored for 10 years after the death of the patient, while other basic medical documentation is to be stored for 15 years.

Due to the lack of clarity with regard to the retention periods of medical records generated during the treatment at health spas, the Information Commissioner, before taking a decision, asked the Ministry of Health for written clarification of whether, in terms of the type of health care provider, medical records processed by natural health spas should be considered part of the patient record and clinical history or part of other basic medical documentation. The retention period for medical documentation is dependent on the definition of its type. The Ministry of Health, after consultation with the Institute of Public Health of the Republic of Slovenia, took the view that the medical documentation generated in health spas should be considered part of the patient record and clinical history, which should be retained for 10 years after the death of the patient.

The Information Commissioner followed the opinion of the line ministry and issued a decision to the responsible entity in which it was ordered to ensure that the personal data of their health service users would be stored and destroyed in accordance with the provisions of ZZPPZ, i.e. 10 years after the death of the user, and that it must ensure traceability of the destruction of personal data of health service users in a way that for every destruction it will be clear when the destruction was carried out and the data of which persons were destroyed (first and last name of the patient, patient record number).

The Information Commissioner concluded that the lack of space and a large quantity of documents in a physical form cannot be a reason for violating the law and for the premature destruction or unlawful processing of personal data. Personal data may in fact be stored in electronic form, as ZZPPZ does not prescribe the form in which health care providers must store records with personal data. Storage of medical records in electronic form solves the problem of lack of space. In addition, such a method of storage makes it easier to search for information or verify what personal data should be destroyed. Also, the destruction of personal data in electronic form is easier than the destruction of documents in physical form. Destruction of personal data prior to the expiration period specified in the sectoral provisions represents a violation of sectoral provisions, and it can also give rise to liability for damages for the data controller for any damage arising from the premature destruction of data.

The Information Commissioner also held that destruction of medical records involves processing of sensitive personal data, which by their nature require consistent implementation of regulatory procedures and measures for their protection. Security of personal data in accordance with Article 24 of ZVOP-1 comprises organisational, technical and logical-technical procedures and measures to protect personal data, prevents accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data by, inter alia (point 5 of paragraph 1), enabling subsequent determination of when individual personal data were entered into a database, when they were used or otherwise processed, and who did so, for the period allowed by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data (internal traceability). Therefore, weighing of the documentation intended for destruction can in no way be sufficient; the responsible entity should ensure that it is clear from the documents prepared at the time of the destruction, when the documents were destroyed and which health service users were included (name and surname of the user, patient record number or treatment number).

Publication of customer personal data on a repairer's „Welcome screen"

During an inspection procedure commenced by the Information Commissioner on the basis of a complaint, it was established that the organisation as the responsible entity was using an electronic booking system and that the following customer personal data appeared on the „Welcome screen": name and surname of the customer, time of admission of the customer, make of customer's vehicle, vehicle registration number, and name and surname of customer's service advisor. Publication on the screen was time-limited and depended on the number of repairs on any given day, on average it lasted one hour per day. When the customer's vehicle went for repair, the screen automatically deleted the customer's data. If the customer did not buy the vehicle through the dealer network and did not sign a contract containing general conditions, the computer program could not detect them, so their name did not appear on the screen.

According to the organisation, the above mentioned screens were intended for customers to see when their vehicle will be accepted for service and which service advisor they should contact. The number of satisfied customers had increased with the introduction of the screen, so in the opinion of the organisation the use of the welcome screen represented a necessary organisational measure that saved customers' time and money, and enabled repair technicians to better prepare for work and thus improved service at the repairer's. In addition, the use of the screen in the manner used by the organisation had also been adopted in other EU countries with comparable legislation in the field of personal data protection. The above mentioned screens have been used by other repairers in the network in other EU Member States since 2004, while in Slovenia they have been in use since 2009.

The Information Commissioner pointed out that the use of a certain technology which incorporates the processing of personal data, must also be considered in terms of the purpose of its use. If the purpose of the data controller is to process personal data of individuals (name and surname of the customer and the vehicle registration number), then by nature this represents processing of personal data for which the processor must have a proper legal basis. A general legal basis for the processing of personal data is defined under Article 8 of ZVOP-1, while the legal basis for the processing of personal data which applies to this organisation is defined in Article 10 of ZVOP-1.

Publication of personal data on the „Welcome screen" represents a communication, dissemination and making personal data available to anyone who is in the premises of the repairer at the time of publication of the data. Such communication, dissemination or making personal data available is certainly not necessary or appropriate for fulfilling contractual or any other obligations of the responsible entity nor is it necessary for the fulfilment of the lawful interests of the private sector, which means that the responsible entity had no legal basis under paragraphs 2 and 3 of Article 10 of ZVOP-1 for the processing (publication) of personal data on the above mentioned screen. Furthermore, the organisation had no basis in law nor the personal consent of the individual for such processing. After reviewing the general terms and conditions for the purchase of a new vehicle and the general conditions for repair of a vehicle, it was established that customers were not aware that their personal data would be processed for the purposes of publication on the „Welcome screen", which means that by publishing customers' personal data on the above mentioned screen the responsible entity acted contrary to the provisions of Articles 8 and 10 of ZVOP-1.

Considering all the above, the Information Commissioner ordered the responsible entity to stop publishing the personal data of its customers – contracting parties (name and surname of the customer with the vehicle's registration number) on its so-called „Welcome screen" in all its service units or instead to obtain express personal consent from each individual customer for the publication of his/her personal data on the „Welcome screen".

Request of an individual to stop the processing of personal data for the purpose of performing chimney sweeping services

In 2013, a procedure was concluded that had been initiated in 2011 following the receipt of a complaint from an individual who had lodged an objection in accordance with paragraph 3 of Article 32 of ZVOP-1 with a data controller (a company that performs chimney services), because the data controller had sent several letters announcing cleaning

services for a solid and liquid-fuel-fired combustion plant at a specific address. The individual argued that no chimney sweeping services had been ordered with the data controller and that no contact had been made with the data controller nor had any information regarding the ownership of property and place of residence of the individual been communicated to the data controller. Therefore, the individual requested the data controller to prove that it was an authorised concessionaire for the provision of chimney sweeping services for the address where the individual had a property, and to prove with an extract from the record of small combustion plants that there was indeed a combustion plant at that location. The individual was of the opinion that the data controller, as a provider of chimney sweeping services, was not entitled or obliged to inspect buildings in search of small combustion plants. Property ownership was not a sufficient basis for the justification of the controller's chimney sweeping services, since the controller would have to demonstrate the existence of small combustion plants at that address, which the controller did not do. This means that the individual's personal data were not used for the fulfilment of the lawful public interest, but exclusively for the interests of the controller who attempted to increase business through general investigation of property owners. Thus, the individual requested the termination of the processing of his personal data.

During the investigation procedure, the Information Commissioner established that the Government of the Republic of Slovenia with Decision No. 35404-31/2007/4 of 8 November 2007 (hereinafter: the Decision) in the area of the Municipality of Kranj, designated the controller as the concessionaire for a period of eight years for the provision of compulsory national public utility services of measurements, inspection and cleaning of combustion plants, flue ducts and vents for the purpose of environmental protection and efficient energy use, protection of human health and protection against fire. The Decision was annulled by the Administrative Court of the Republic of Slovenia with its judgement no. U 2354/2007-13 of 5 November 2008 (hereinafter: the Judgement) and remitted to the Government for reconsideration, which at the time the Commissioner initiated the investigation procedure, had not yet issued a new decision. Therefore, the individual claimed that the controller did not have a concession for the provision of chimney sweeping services in the area where his two properties were located.

On the basis of the allegations in the complaint, during the procedure the Information Commissioner examined whether the data controller was processing the individual's personal data (name, surname and address) in accordance with paragraph 3 of Article 10 of ZVOP-1, namely because this would be necessary for the fulfilment of the lawful interests of the private sector (the controller) and these interests would clearly outweigh the interests of the individual to whom the personal data relate. An individual whose personal data are being processed in accordance with paragraph 4 of Article 9 or paragraph 3 of Article 10 of ZVOP-1 has the right by objection at any time to demand the cessation of their processing. The data controller shall grant the objection if the individual demonstrates that the conditions for processing have not been fulfilled pursuant to the above articles. In this case the personal data of the individual may no longer be processed (paragraph 3 of Article 32 of ZVOP-1). If the data controller does not grant the objection, the individual may request that the Information Commissioner decides on the data processing.

For the Information Commissioner the key question was whether the processing of personal data by the controller is lawful. Thus, the Information Commissioner requested the Ministry of the Environment and Spatial Planning to clarify whether the controller as the holder of the concession had legal basis for the provision of compulsory public utility services and could therefore be regarded as a controller – i.e. an entity that legally obtains and further processes personal data of individuals with whom it enters into a contractual relationship under the obligation to contract (compulsory public utility service), and if so, what this legal basis was. The Ministry made it clear that the Decision was annulled, but that the concession contract was still in force, because there were no circumstances for its rescission under the current legislation.

Taking into consideration the Ministry's clarification, the Information Commissioner concluded that despite the Judgement the controller was lawfully carrying out chimney sweeping services. In Article 148 of the Environmental Protection Act the legislator provided that chimney sweeping services are one of the mandatory national public utility services in the field of environmental protection. In accordance with said Article, the Government issued a Decree on the method, subject and conditions for the performance of the compulsory

public utility service of measurement, inspection and cleaning of combustion installations, flue ducts and ventilation shafts for the purpose of environmental protection and efficient use of energy, health protection and fire protection, which provides that chimney sweeping services are performed by way of concession, namely one exclusive concession is granted for an individual area, which means that only the selected concessionaire may provide chimney sweeping services therein. Slovenia is divided into 194 zones for chimney sweeping services. ZVO determined that the chimney sweeping services for small combustion plants are carried out for the public interest, i.e. for reasons of environmental protection, efficient energy use, protection of human health and protection against fire.

In accordance with Article 5 of the Public Utilities Act, the use of public resources which are ensured by compulsory public utility services, is obligatory, if the law or a regulation issued on the basis thereof does not, in individual circumstances, provide otherwise. According to paragraphs 1 and 2 of Article 6 of the Decree, the use of chimney sweeping services is obligatory for all users of chimney sweeping services. Users of chimney sweeping services are defined as persons who control and use small combustion plants, auxiliary devices, flue ducts or vents, or as property owners, if user status could not be determined under the previous criteria. In accordance with Article 29 of the Decree, users of chimney sweeping services must enable unobstructed and safe operation of chimney sweeping services, provide unhindered and free access to combustion plants, flue ducts, auxiliary devices or vents to the concessionaire on the agreed date, allow viewing of the plans of these devices and allow access to areas where devices are located or through which they are routed, that is to areas in which chimney sweeping services are carried out, as well as allow viewing of the plans of the building in which these devices are installed or through which they are routed. If users fail to fulfil their obligations, the concessionaire shall notify the inspectorate responsible for environmental protection. The inspector may order the user to provide everything necessary for the performance of chimney sweeping services.

It is clear from the cited legal bases that users are obliged to use chimney sweeping services, even if they only act in their capacity as owners of the property, and that chimney sweeping services for small combustion plants are carried out as a compulsory public utility service in the public interest, the implementation of which must be provided by the state.

The Information Commissioner therefore concluded that paragraph 3 of Article 10 of ZVOP-1 was not the legal basis for the processing of personal data of the individual by the controller, since that provision only applies when the controller demonstrates a necessity to process personal data for the fulfilment of lawful interests of the private sector and has no legal basis for the processing of certain personal data in the law, no personal consent nor contractual relationship. The basis for the processing of personal data of the individual in this case is paragraph 1 of Article 10 of ZVOP-1, in conjunction with Article 148 of ZVO because it regards a public utility service in the public interest, despite the fact that ZVO does not specify precisely the processing of personal data nor the set of personal data to be used for the purpose of carrying out chimney sweeping services. In the case of the provision of compulsory public utility services in the field of chimney sweeping services, the user (individual as the property owner) is in a forced relationship with the concessionaire – chimney sweeping service providers (controller) as required by ZVO and the Decree. The processing of certain personal data of the user (personal name and address) is merely a consequence of this forced relationship established by law for the purpose of fulfilment of the public interest, as it is recognized and codified by ZVO. For this purpose (service announcement to check whether the individual has a small combustion plant or not and to provide chimney sweeping services) the public utility service provider may in accordance with paragraph 1 of Article 10 of ZVOP-1 process certain personal data of users, which are for the same purpose obtained from public records and books. In accordance with the provisions of Article 38 of the Decree, concessionaires must also keep records of their services performed on small combustion plants, flue ducts, vents and auxiliary devices, and records of measurements of gaseous emissions from small combustion plants.

Considering the above, the Information Commissioner adopted a decision rejecting the individual's objection, as in the case of the processing of personal data pursuant to paragraph 1 of Article 10 of ZVOP-1 individuals do not have the right to request cessation of the processing of their personal data.

The individual initiated an administrative dispute against the decision of the Information

Commissioner, filing an action before the Administrative Court of the Republic of Slovenia. The Administrative Court dismissed the action, establishing that the procedure prior to the issuance of the contested decision was correct, as was the decision of the Information Commissioner. The individual lodged an appeal on points of law against the judgement of the Administrative Court before the Supreme Court of the Republic of Slovenia, which dismissed the appeal as unfounded.

4.3. General Assessment of the status of Personal Data Protection and Recommendations

In 2013, the Information Commissioner conducted 712 inspection procedures, of which 253 pertained to the public sector and 459 to the private sector (725 in 2012, 682 in 2011, and 599 in 2010), and 106 minor offence procedures (158 in 2012, 136 in 2011, and 179 in 2010) regarding personal data protection.
In addition to inspections and minor offence procedures, in 2013, the Information Commissioner received 2,460 requests for an opinion or an explanation in relation to personal data protection (2,191 such requests in 2012, 2,143 in 2011, and 1,859 in 2010), six requests for permission to link databases of personal data (9 in 2012, 14 in 2011, and 9 in 2010), 11 applications for permission to implement biometric measures (11 in 2012, 9 in 2011, and 6 in 2010), 14 requests for authorisation of a transfer of personal data to third countries (5 in 2012, 4 in 2011, and 8 in 2010), 68 appeals against refusals to allow access to one's personal data (63 in 2012, and 85 in 2011 and 2010) and 11 appeals against refusals of requests for information under the Patient Rights Act (10 such complaints in 2012).
In mid-June 2013, the provisions of Article 157 of ZEKom-1 on cookies which relate to the retention of information or the gaining of access to information stored in a subscriber's or user's terminal equipment, entered into force. After the provisions of Article 157 of ZEKom-1 came into effect, the Information Commissioner, as the body responsible for monitoring and inspection of the implementation of those provisions, had, by the end of 2013, received 35 complaints relating to 141 responsible organisations (website operators). Complaints were mostly related to inadequate or no notice and inappropriate mechanisms for obtaining consent. The vast majority of responsible organisations against which the Information Commissioner initiated inspection procedures corrected the identified irregularities or violations upon being informed of them, thus the Information Commissioner was not required to issue regulatory decisions.

The Information Commissioner notes that the number of complaints regarding suspected infringements of regulations received each year has diminished and is no longer increasing as it did in previous years. This also applies to other applications or requests received with regard to personal data protection each year. Due to the somewhat fewer number of complaints, the Information Commissioner was able to devote more attention in 2013 to so-called planned ex officio inspections, which are carried out in accordance with the Commissioner's agreed annual plan.
In addition to complaints filed in the relevant period in connection with cookies, in 2013, as in previous years, the largest number of complaints received by the Information Commissioner related to video surveillance and the use of personal data for direct marketing purposes. Apart from the above mentioned complaints, particular attention must be drawn to complaints that were filed regarding the transfer and, consequently, reading of e-mails sent to company e-mail addresses of employees; complaints that were filed regarding the publication of personal data on the websites of data controllers; complaints that were filed regarding the sending of payable SMS messages; and complaints that were filed regarding the processing of inaccurate and outdated data.
During its consideration of complaints, the Information Commissioner discovered that after termination of employment of an employee, employers often do not cancel or delete the company e-mail address used by that former employee, but instead simply redirect e-mail that is sent to the former employee's company e-mail address to another employee's e-mail address. Such conduct does not only represent unlawful use of personal data (e-mail address of an employee), but it also enables the person to whom received e-mail is redirected to be unlawfully familiarised with the personal data of third parties, i.e. people who send e-mails to the e-mail address of a former employee (informed of their

email addresses, traffic data and the content of sent messages). Employers justify such conduct arguing that in this way a continuous business process is ensured and they avoid damage to the business arising from the possible loss of an order. Such a justification can in no way be considered adequate as employers can also ensure a continuous business process very simply and without unlawful processing of personal data or breach of the so-called communication privacy of individuals, which can also represent a criminal offence of violation of the confidentiality of communications under Article 139 of the Penal Code. One of the simple ways to avoid unlawful processing of personal data after the termination of employment of an employee, while at the same time ensuring a smooth continuation of the business process, is for example to provide, for a limited time, an automated return message for the cancelled e-mail address informing the sender that the e-mail address is no longer active and that business e-mails should be sent to another e-mail address. The same applies in the event of a prolonged absence of an employee, in which case redirection of e-mail to another address is not permitted, even if the individual to whom the e-mail address belongs gives their personal consent. It should be noted that by redirecting e-mail to another person, not only personal data of the individual to whom the e-mail address belongs are disclosed, but also the personal data of individuals who send e-mails, which are subsequently redirected, are disclosed.
When considering complaints regarding the publication of personal data on websites of data controllers, the Information Commissioner established that data controllers publish personal data on their websites mainly due to negligence, which nevertheless does not justify their conduct. Such publication most frequently occurs because controllers do not have procedures and measures in place to ensure that, prior to the publication of particular material, it is appropriately checked to determine whether the material to be published contains personal data which should not be publicly available. The Information Commissioner therefore calls upon website operators to avoid such breaches by establishing and ensuring appropriate organisational and technical procedures and measures to be able to successfully prevent such unlawful disclosure of personal data.

During the relevant period, the Information Commissioner also received several complaints regarding payable SMS messages sent by the Austrian company Dimoco. In its consideration of these complaints, the Information Commissioner did not find elements of violation of the provisions of ZVOP-1, and was only able to establish unfair commercial practice of the company, which consumers are also being warned about by the Slovenian Consumers` Association through its websites. Investigation shows that these company's web pages offer a variety of content (e.g. IQ tests, various games, etc.). When individuals want to obtain the result for example of the IQ test, they have to enter their mobile phone number in a special box on the web page, and with the subsequent window on the website, where they enter a code received via SMS message, they (usually unknowingly) become a member of the SMS-club. The fact that one has in this way joined the SMS-club, is only noticed by the individual after receiving a higher monthly bill from their mobile phone operator. By becoming a member of the SMS-club, an individual agrees to receiving text messages from the provider at a price of 2.49 EUR/SMS, which significantly increases their monthly phone bill. The Information Commissioner therefore recommends that individuals, prior to transmitting or entering their phone numbers when solving various tests or playing various games, carefully read the rules, which are often contained in the fine print or on subpages, and that in the case of receiving a suspicious SMS message they carefully read that message and they, depending on its content, do not respond to it or immediately cancel the receipt of ordered payable messages.

Due to misinterpretations of the provisions of ZVOP-1, each year the Information Commissioner receives many complaints from individuals claiming that a certain data controller has personal data relating to them which is incomplete, inaccurate or outdated. In connection with such complaints it is necessary to clarify that the Information Commissioner is not competent to judge whether the controller keeps accurate and up-to-date personal data on a particular individual. Individuals who believe that a certain controller has inaccurate or outdated personal data on them are therefore advised to first lodge, in writing (by registered mail or with acknowledgement of receipt), a request with the data controller under Articles 30 and 31 of ZVOP-1 for a viewing of, transcription of, or printout of their personal data as well as information on the sources of such data. On the basis of such data and information an individual will be able, in accordance with Articles 32 and 33 of ZVOP-1, to request the data controller to supplement, correct, block or erase personal data which the individual proves as being incomplete, inaccurate or not up-to-

date, or that they were collected or processed contrary to legislation. If the data controller refuses the individual's request to supplement, correct, update or erase personal data, the individual cannot exercise their rights with the Information Commissioner, but may on the basis of Articles 34 and 35 of ZVOP-1 request judicial protection in the Administrative Court of the Republic of Slovenia. The Information Commissioner may, in respect of an individual's refused request to supplement, correct, block or erase personal data, only take action if the data controller does not decide on the individual's request within 15 days and does not inform the individual of the decision, and if an individual's personal data are being processed unlawfully (without a basis in law or personal consent of the individual). Data controllers are therefore reminded that, in the case of an individual's request for familiarisation with their personal data under Articles 30 and 31 of ZVOP-1 and in the case of an individual's request to supplement, correct, block or erase personal data under Articles 32 and 33 of ZVOP-1, they are required to grant the individual's request and inform the individual of same in writing within the legally stipulated time period, or if the request is not granted, notify the individual in writing of the reasons for the refusal within the same period.

An important part of the activities of the Information Commissioner also relates to the introduction of new powers granted to law enforcement authorities, particularly with regard to very frequent changes in the regulation of criminal proceedings. The Information Commissioner notes that there are still many difficulties in interpreting communication privacy, and points out that neither a written request from a state authority nor a court order is sufficient to obtain information on the identification of communicating individuals, as this area falls within the provisions of Article 37 of the Constitution of the Republic of Slovenia. The Article provides that the confidentiality of correspondence and other means of communication shall be guaranteed and that only on the basis of a court order may the protection of the confidentiality of correspondence and other means of communication and the inviolability of personal privacy be suspended where such is necessary for the initiation or during the course of criminal proceedings or for reasons of national security. Thus the Constitution of the Republic of Slovenia sets strict conditions for the intrusion into communication privacy, including judicial review, and clearly this was another attempt to avoid this. At the end of 2013, the Information Commissioner published a report which revealed disturbing practices of the police, who in 2012, despite the clear provisions of the Electronic Commerce Market Act and the Criminal Procedure Act, on the basis of 35 written requests, requested data from information society service providers concerning users of websites with content that is supplied or transmitted by users of the service. In 31 cases, this was done without the necessary court order, while 30% of written requests did not qualify the criminal offence in question. It is also evident that there is a lack of knowledge of the differences between operators (providers of publicly available electronic communications networks and services) whose operation is primarily governed by ZEKom-1 and operators of websites (information society service providers) whose operation is primarily governed by ZEPT. If the police requests traffic data (data on IP-address) from information society service providers, they can only request this information from operators on the basis of paragraph 1 of Article 149.b of ZKP, which requires a court order. If they request information from information society service providers who are not operators, they also require a court order, as stipulated in paragraph 4 of Article 8 of ZEPT.

In addition to the trends that were discussed in the previous report (cloud computing, so-called "big data"), new challenges for personal data protection continue to be present in the field of modern information and communication technologies. This mainly concerns the wider use of remotely piloted automated systems, which enable the concealed, difficult to detect and extensive collection of personal data and significant invasions of privacy. Since these remotely piloted automated systems can be equipped with a wide variety of sensors that enable capture of videos, images, sound and data on temperature, movement, location, etc., their use will represent a major challenge for the regulators as well as the guardians of privacy.

The Information Commissioner notes that personal data database controllers are fully familiar with the requirements of ZVOP-1 and that the activities of the Information Commissioner in the areas of raising awareness and inspection are efficient. In other countries a large number of large-scale abuses, including losses of enormous amounts of personal data have occurred. In Slovenia, such large-scale violations have not been identified, and here we also have to take into account the fact that such major violations

almost never remain undetected.

Regarding the use of information systems in which personal data are processed, a major emphasis remains on ensuring that the requirements of personal data protection are complied with at an early stage, by means of preliminary assessments of impacts on privacy, which enable the timely identification and reduction of risk of misuse of personal data. The Information Commissioner notes that their usefulness is still not recognised enough. It would be appropriate to devote additional efforts to better raise the awareness of certain professional profiles, such as system and application developers, IT experts and experts in the field of electrical engineering, as by taking into consideration the Privacy by Design principle, many abuses of the fundamental principles of personal data protection, especially problems of legality, proportionality and information security, could be prevented.

Due to limited staff resources, complaints filed in the relevant period in relation to cookies were classified and dealt with by the Information Commissioner on the basis of priority, based on criteria of importance/visibility of individual websites and the assessed severity of the invasion of privacy. When considering complaints, the Information Commissioner found that violations of the provisions of Article 157 of ZEKom-1 were quite common in practice. Websites consistently informed their customers about the use of cookies, but did not always provide adequate control mechanisms that would actually allow or prohibit the installation of cookies. In particular, there were several cases where a website installed cookies, for which following the entry into force of said Article 157, explicit consent of the user is required, upon the first visit to the website, as well as cases where a website operator interpreted the provisions of paragraph 2 of Article 157 of ZEKom-1, covering exceptions (strictly necessary cookies) for which no consent is required, too broadly. The Information Commissioner is pleased to note that in the majority of cases operators were willing to eliminate these deficiencies immediately upon receipt of the Information Commissioner's notice, therefore, before the issuance of a final decision. Especially problematic were advertising and analytical cookies, but also cookies of certain plug-ins that are as a general rule installed by third parties and that allow recording of the user's everyday on-line activities across several different websites ("tracking cookies"). So in cooperation with responsible entities the Information Commissioner developed Guidelines for the use of cookies and answers to frequently asked questions, which were posted on the Information Commissioner's web pages. The Information Commissioner received many questions from website operators about web analytics, namely how to implement it so that it would be allowed on the basis of presumed consent and at the first visit. The Information Commissioner achieved the withdrawal of some of the more invasive plug-ins, primarily in respect of public sector websites and major Slovenian media websites.

The Information Commissioner actively monitors developments in connection with the reform of the legislation on personal data protection in the EU, and was actively involved with the Future of Privacy subgroup. According to the Information Commissioner, some of the solutions envisaged, such as greater emphasis on persons responsible for personal data protection, assessment of impact on personal data protection and certification, represent more effective measures for personal data protection. Of particular importance will be the question of responsible entities and the territorial scope of future legislation, as some of the very large data controllers, such as Google and Facebook, are currently only bound to a limited extent by the provisions of the European legislation.

An area which has also attracted greater attention in the global context is the operation of security and intelligence services. In particular, Snowden's revelations regarding the US National Security Agency (NSA) have caused a wave of outrage and questions about who and to what extent they are intruding into our privacy. Following Edward Snowden's revelation of the total control over Internet data, telecommunications operators in the United States of America and data which are in vast quantities supplied to Google cloud platform, Facebook, Microsoft, Amazon, etc., also by Europeans, a special ad hoc EU–USA group was set up with the task of establishing the actual state of NSA activities regarding mass collection of information and personal data of EU citizens. As one of the five top European experts in the field of personal data protection,.head of the Information Commissioner Nataša Pirc Musar, was appointed a member of the said group by the European Commissioner.

5 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

5.1. Participation in the Preparation of Legislation and other Regulations

In accordance with the provisions of Article 48 of ZVOP-1, the Information Commissioner issues preliminary 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 acts and other regulations with the acts and other regulations regulating personal data processing.

In 2013, the Information Commissioner detected a disturbingly large number of amendments to acts and proposals for new acts, which would enable serious intrusions on the privacy of individuals in terms of the processing of personal data, which are being adopted using fast-track procedures without appropriate analyses and assessments of their consequences for ensuring the constitutionally guaranteed protection of privacy and personal data of individuals.

In 2013, the Information Commissioner received 106 requests for an opinion on proposals for acts and other regulations. The Information Commissioner, inter alia, provided opinions on proposals for the following acts:

- proposal for the Act Amending the Subsidised Student Meals Act (opinion of 19 December 2013);
- initiative for the conclusion of the Agreement between the Government of the Republic of Slovenia and the Council of Ministers of Bosnia and Herzegovina on collaboration in the work of joint investigation teams, cross-border secret surveillance or tracking, sending and comparison of DNA profiles and other identification materials and with liaison officers (opinion of 16 December 2013);
- proposal for amendments to the Criminal Procedure Act (opinion of 12 December 2013);
- proposal for The Removal and Transplantation of Human Body Parts for the Purposes of Medical Treatment Act (opinions of 16 August and 11 December 2013);
- initiative for the conclusion of the Agreement between the Government of the Republic of Slovenia and the Government of Montenegro on collaboration in the work of joint investigation teams, cross-border secret surveillance or tracking, sending and comparison of DNA profiles and other identification materials and with liaison officers (opinion of 10 December 2013);
- proposal for amendments to the Electronic Commerce Market Act (opinion of 27 November 2013);
- proposal for the Act Amending the Aliens Act (opinion of 22 November 2013);
- draft amendments to the legal basis for the system of information on the credit standing of clients and the exchange of personal data on disputable circumstances (opinion of 8 November 2013);
- proposal for amendments to the Courts Act (opinions of 6 November and 12 December 2013);
- proposal for the Gaming Act (opinion of 22 October 2013);
- proposal for the Prevention of Undeclared Work and Employment Act (opinion of 14 October 2013);
- proposal for the Act Amending the Health Care and Health Insurance Act (opinion of 17 October 2013);
- General Act of Data Retention on the basis of paragraph 4 of Article 165 of the Electronic Communications Act (opinion of 3 September 2013);
- the proposal for the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Kosovo on police cooperation (opinion of 26 August 2013);
- proposal for the Agreement between the Government of the Republic of Slovenia and the Government of the Republic of Macedonia on police cooperation (opinion of 21 August 2013);
- proposal for the Regulations on the implementation of article 153 of Electronic Communications Act (opinions of 28 June and 21 August 2013);
- proposal for the Rules on the processing of data on electronic communications of the Police and on access to police databases (opinion of 12 August 2013);
- proposal for a regulation of the European Parliament and of the Council concerning homologation for the deployment of the eCall in-vehicle system and for an amendment to Directive 2007/46/EC (opinion of 6 August 2013);

- proposal for the Parental Protection and Family Benefit Act (opinion of 18 July 2013);
- initiative for the conclusion of the Agreement between the Ministry of the Interior of the Republic of Slovenia and the Federal service of the Russian Federation for narcotics traffic control, on cooperation in combating illicit traffic of narcotic drugs, psychotropic substances and their precursors (opinion of 18 June 2013);
- proposal for the Act Amending the Minor Offences Act (opinion of 13 June 2013);
- initiative for the conclusion of the Agreement between the Government of the Republic of Slovenia and the Government of the United States of America on improving international tax compliance and implementation of FATCA (opinion of 10 May 2013);
- proposal for the Voting Rights Register Act (opinion of 7 May 2013);
- proposal for the Regulation on Europol (opinion of 6 May 2013);
- proposal for the Rules on the equipment and interfaces for lawful interception of communications (opinion of 29 April 2013);
- proposal for the Rules on the method of transmitting retained data on the traffic of telephone and data services in mobile and fixed electronic communications networks (opinion of 26 April 2013);
- Act Amending the Patient Rights Act (opinion of 20 March 2013);
- proposal for a directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (opinion of 8 March 2013);
- the position of the Information Commissioner regarding the introduction of a new definition of pseudonymous data in the proposed reform of personal data protection in the EU (opinion of 5 March 2013);
- proposal for the Act Amending the Insurance Act (opinion of 11 February 2013);
- proposal for the Rules on requirements for computer programmes and electronic devices, management and operation of the information system and the content, form, manner and deadlines for the submission of the documents referred to in paragraph 11 of Article 38 of the Tax Procedure Act (opinion of 11 February 2013).

5.2. Relations with the Public

Throughout 2013 the Information Commissioner was committed to ensuring the public nature of its work and raising 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) and through its website. In 2013, the Information Commissioner also communicated via the on-line social network Facebook, where through its profile it raises awareness of the importance of personal data protection.

The Information Commissioner was also actively involved in the Council of the SAFE-SI project and Spletno oko, which operate in the field of safe use of the Internet. Within the framework of this activity it conducted numerous lectures on the protection of personal data on the Internet for pupils, teachers and parents.

Through various workshops and seminars the Information Commissioner provided for the continuing education of responsible entities. It also participated in various educational conferences, workshops and round tables.

In 2013, the Information Commissioner prepared an special event on the occasion of European Data Protection Day (28 January), with which it wanted to draw attention to the safe use of smart mobile devices. Many people today can no longer imagine life without smart mobile devices. We want to be connected, available and sociable at all times. But is this safe? And what does this mean for our privacy? The central part of the event were a round table and a presentation of the guide entitled "ABC of security and privacy on mobile device" (ABC varnosti in zasebnosti na mobilnih napravah), which is the result of a collaboration between the Information Commissioner and the awareness-raising programme Safe on the Internet (Varni na internetu) of the Slovenian Computer Emergency Response Team (SI-CERT), which operates under the auspices of the public institution Arnes. The said guide describes problems or abuse that may occur in the world of mobile devices

and gives recommendations for the safe use of mobile applications and devices. Mobile devices are minicomputers with all the functionality, but unfortunately also with all the nuisances of the web. Viruses, abuse and invasions of privacy are a reality, which is why the Information Commissioner and experts who participated in the round table drew attention to the fundamentals of safe use of smart devices and pointed out that smart devices are only as smart as their users.

As is tradition, we took this opportunity to award good practice in the field of personal data protection. In the private sector, the award was given to Zavarovalnica Maribor, d. d., where the importance of the personal data protection is integrated in the system of work and is reflected both in the minds of employees as well as in technical solutions to prevent potential abuses. In the public sector, the award was given to the Supreme Court of the Republic of Slovenia, which, with its responsiveness and inclination towards the protection of personal data and privacy of individuals in the case of the electronic land register (e-ZK), demonstrated that even the most rigid and precise statutory provisions can be used hand in hand with the principle of proportionality. Recognition was also given to companies that acquired certification under the information security standard ISO/IEC 27000 in 2012, demonstrating a high level of protection of personal data (Inštitut za nutricionistiko, 3GEN, d. o. o., iPLUS, d. o. o., Elektro Slovenija, d. o. o., GENIS, d. o. o., MICROCOP, d. o. o., Agencija za trg vrednostnih papirjev, HSE Invest, d. o. o., Loterija Slovenije, d. d.).

The Information Commissioner gave special recognition, with the title Ambassador of Privacy 2013, for efforts in the field of the so-called privacy by design, to the IT and e-Services Directorate at the Ministry of Justice and Public Administration, namely for consideration of privacy by design in its successful work on European projects STORK, SPOCS, STORK 2.0 and others as well as in preparing the analysis of options for the introduction of safer and user-friendly e-identities.

World Right to Know Day is celebrated each year on 28 September, ever since various civil society organisations from many countries connected to form the Freedom of Information Advocates Network (FOIAnet) in 2002. On 30 September 2013, on the occasion of the World Right to Know Day, the Information Commissioner organized a working conference regarding the implementation of ZDIJZ. Nataša Pirc Musar, Head of the Information Commissioner, and mag. Goran Klemenčič, chairman of the Commission for the Prevention of Corruption, presented developments in this field, planned changes in legislation, and the role and importance of transparent operation to prevent corruption and build integrity. Participants were presented examples of good practice in the implementation of ZDIJZ by representatives of responsible authorities, while representatives of the applicants (journalists and non-governmental organizations) highlighted the problems they were facing in practice.

On 24 October 2013, the Information Commissioner organised an international conference on the theme of re-use of public information. The conference was organised within the framework of the European LAPSI project (Legal Aspects of Public Sector Information; http://www.lapsi-project.eu/), which is intended to establish a thematic network in the field of re–use of public information and is funded by the European Commission, and where the Information Commissioner as one of its partners cooperates. The purpose of the conference held in Ljubljana was to present new trends and challenges brought by the amendment to Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re–use of public sector information. The event was also broadcast live over the Internet.

In 2013, the Information Commissioner also continued with preventive work and prepared Guidelines on intelligent video analytics and Guidelines on the use of cookies on websites.

Public Opinion Research Center Politbarometer carried out several surveys in 2013 within the framework of the project Public opinion polls on the attitude of the public towards the current situation and developments in Slovenia. A public opinion poll conducted in January 2013 also included an assessment of the performance of the national supervisory authorities. The authorities assessed included the Information Commissioner, the Ombudsman, the President of the Court of Auditors, the Governor of the Bank of Slovenia and President of the Commission for the Prevention of Corruption. The public opinion poll indicated that their performance was assessed as extremely and highly positive by respondents (as

opposed to the assessment of the functioning of the central state bodies (the National Assembly, the Government, the President of the Government). Head of the Information Commissioner Nataša Pirc Musar was ranked at the very top. It should not be overlooked that the Information Commissioner also ranked highest among the central government and social institutions most trusted by Slovenians in public opinion polls in 2010, 2011 and 2012, which shows an established confidence of people in the work of the Information Commissioner.

In October 2011 in Ottawa, Canada, the community of information commissioners and similar institutions responsible for transparency and protection of the right of access to information, decided to create and present to the public a joint website of all information commissioners. This demanding task was entrusted to the Slovenian Information Commissioner, who took over the project and created info-commissioners.org. The Information Commissioner was also responsible for the operation of this website in 2013.

5.3. International Cooperation

As the national supervisory authority for the protection of personal data, the Information Commissioner regularly cooperates with the competent bodies of the European Union (EU) and the Council of Europe for personal data protection. Cooperation at an international level and participation in EU legislative procedures is also dictated by Directive 95/46/EC.

Due to budgetary cuts, in 2013 the Information Commissioner participated in only the most urgent European Union plenary meetings and occasionally attended meetings of four of the many subgroups of the Article 29 Working Party. In total, the Information Commissioner participated in eight EU working bodies dealing with control over the implementation of personal data protection in the context of individual areas of the EU, namely:

- theWorking Party for personal data protection under Article 29 of Directive 95/46/EC, as well as four of its subgroups (the Future of Privacy Subgroup, the Technology Subgroup, the Binding Corporate Rules (BCR) Subgroup, and the Borders, Travel and Law Enforcement (BTLE) Subgroup);
- the Europol Joint Supervisory Body;
- the Joint Supervisory Authority for Schengen;
- the Joint Supervisory Authority for Customs;
- at coordination meetings of the European Data Protection Supervisor together with national authorities for the protection of personal data for the supervision of SIS II;
- at coordination meetings of the European Data Protection Supervisor together with national authorities for the protection of personal data for the supervision of CIS;
- at coordination meetings of the European Data Protection Supervisor together with national authorities for the protection of personal data for the supervision of VIS;
- at coordination meetings of the European Data Protection Supervisor together with national authorities for the protection of personal data for the supervision of EURODAC.

In March 2013, the Head of the Information Commissioner was elected Chairman of the Europol Joint Supervisory Body. The Information Commissioner also actively participated in the International Working Group on Data Protection in Telecommunications (IWGDPT), which brings together representatives of Information Commissioners and authorities for personal data protection and privacy from around the world. Once again in 2013, a representative of the Information Commissioner participated in the Council of Europe's Consultative Committee (T-PD) on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

On 19 July 2013, Head of the Information Commissioner Nataša Pirc Musar was appointed by the European Commission to a special ad hoc EU–USA group, whose task was to determine the actual level of activity of the US National Security Agency (NSA) in relation to mass collection of information and personal data of European Union citizens. Nataša Pirc Musar participated in the special group as one of the five top European experts in the field of personal data protection. At the end of its mandate, the group prepared a report on its findings for the European Commission.

On the basis of Article 60 of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System and Article 44 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), the Information Commissioner is responsible for independent monitoring of the lawfulness of the processing of SIS II personal data in their territory and its transmission from their territory. In 2013, the Information Commissioner received no complaints regarding the implementation of these rights in the first instance.

In 2013, the Republic of Slovenia conducted an evaluation of the implementation of the Schengen acquis in terms of personal data protection, in which the Information Commissioner actively participated.

In 2013, the Information Commissioner hosted representatives of similar institutions from Croatia, Bosnia and Herzegovina and Macedonia. They were familiarised with its operation and good practice in the areas for which it is responsible.

In 2013, the Information Commissioner as a leading partner successfully completed Twinning Light Project SR/2009/IB/JH/01 – "Improvement of Personal Data Protection" in Serbia. In the context of international cooperation in the field of access to public information, in 2013 the Information Commissioner began a two-year participation in an international consortium in the LAPSI 2.0 project, which is intended to continue the work of the LAPSI 1.0 project and to establish a thematic network of experts in the field of the re-use of public information with the objective to remove obstacles to its implementation that occur in practice.

Editor:

Nataša Pirc Musar

Authors:

dr. Monika Benkovič Krašovec, State Supervisor for the Protection of Personal Data
Jože Bogataj, Head of State Supervisors for the Protection of Personal Data
Jasna Duralija, Advisor
Alenka Jerše, Secretary General
Eva Kalan, Advisor
Kristina Kotnik Šumah, Deputy Information Commissioner
Blaž Pavšič, State Supervisor for the Protection of Personal Data
mag. Andrej Tomšič, Deputy Information Commissioner

Design:

mag. Matjaž Drev and Bons, d. o. o.

Informacijski pooblaščenec Republike Slovenije
Zaloška cesta 59
1000 Ljubljana

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

Ljubljana, May 2014

ISSN 1854-9500