INFORMATION COMMISSIONER

OF THE REPUBLIC OF SLOVENIA

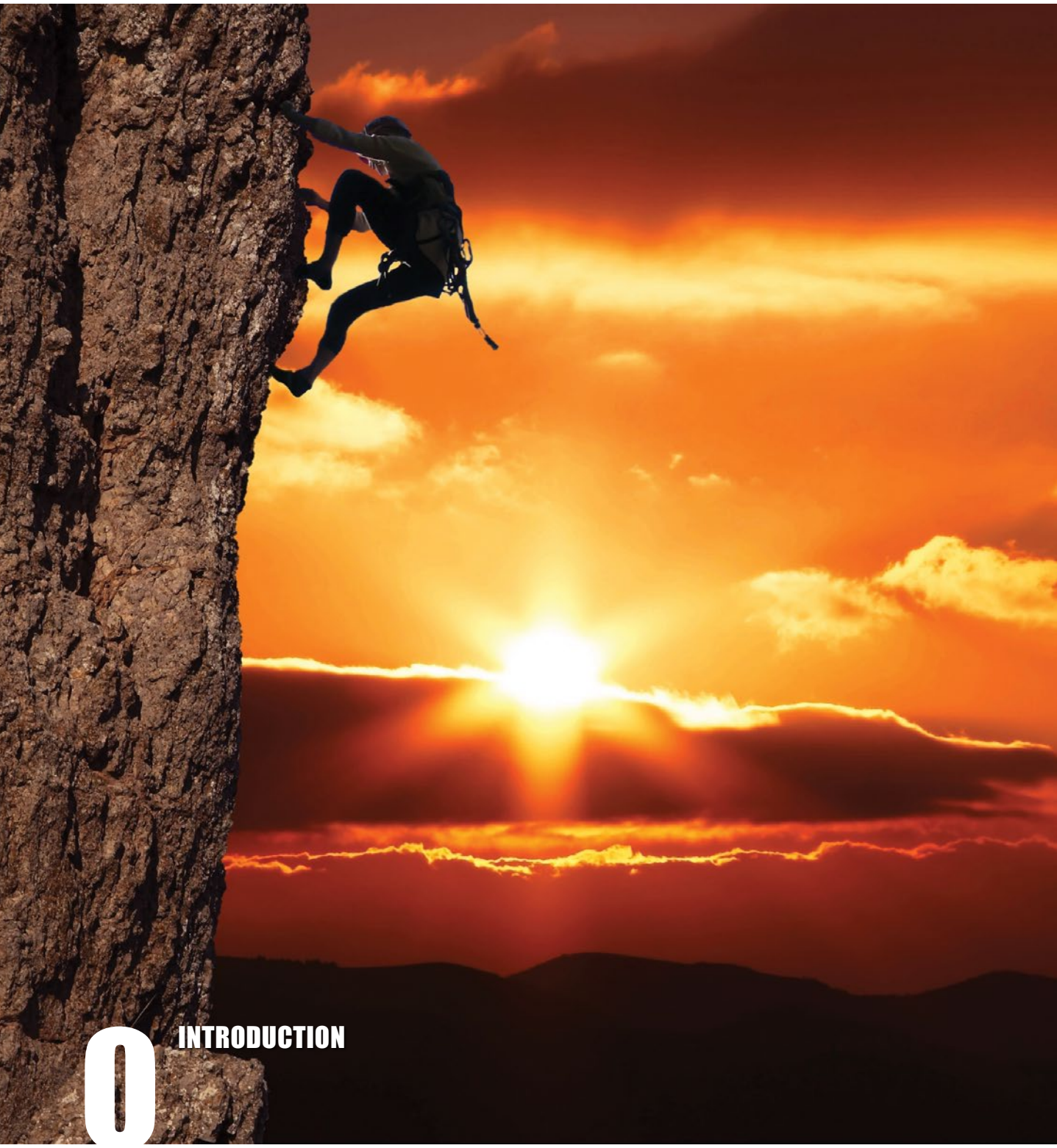
'12 Annual Report Information Commissioner

2012

'12 Annual Report

Information Commissioner

2012



0 INTRODUCTION

We could mark the year 2012 as a year of ambitious plans of the state for additional informatization of large public data bases following an expeditious procedure, and the growth of the appetites of the public sector for ever more expanding processing of personal data. Foremost it is alarming that the state that should have been protecting privacy according to the Slovenian Constitution is starting to erode the privacy foundations.

The Information Commissioner dealt with more than 80 proposals for amendments to legislation, that provide for personal data collection and processing, which is more than a third more than in the 2011. Many of the proposals are, in our opinion, an attempt to legalise disproportionate collection and processing of personal data that will neither contribute to administrative procedures being simpler nor to the austerity measures, but will on the other hand lower the level of privacy protection of citizen. Among the acts that have been in the process of amendments are the Electronic Communications Act, Act on Police Tasks and Authorities, Labour Market Regulation Act, Inheritance Act, Public Procurement Act, Public Administration Act. Most of the proposals for amendments show a complete lack of data protection impact assessments that should have been presented in the context of new planned data processing activities. It seems that the financial crisis has not touched the informatization area as much as other parts of the public sector. On contrary, many of the intended informatizations will bring considerable costs.

The Information Commissioner dealt with an extremely high number of cases in the two fields of operation, regarding either requests for an opinion, complaints, or appeals. Such circumstances are on the one hand positive, being evidence that individuals are ever better informed and having increased awareness and understanding of the purpose and importance of these two human rights whose implementation and protection fall within the competence of the Information Commissioner. At the same time, such increase in the number of appeals and cases related to inspections has to be ascribed also to certain worrisome actions of liable authorities in the area of access to public information, on the one hand, as well as to the enormous (perhaps too enormous) appetites of various data controllers from the private and public sectors as regards processing personal data.

Regardless of the increasing number of cases, the Information Commissioner strives for an increasing level of responsiveness and professionalism; however, due to the increasing number of cases processed this is barely still attainable. Nevertheless, I am pleased that in 2012 we again succeeded in doing so and that the public recognises our efforts to protect both fundamental rights, i.e. the right to access public information and the right to personal data protection, and thus in the past year it again expressed a high level of trust in the Information Commissioner.

According to research carried out by the Public Opinion and Mass Communication Research Centre, as of January 2013 the level of trust in the Information Commissioner was characteristically high again (52%), the highest among the examined 4 supervisory institutions. Since previous measurements also demonstrated a high level of trust and since the percentage has always been in the upper half of the range, a continuous level of trust has clearly been expressed, which makes me extremely satisfied and at the same time compels us to continue with our work and seek ways to improve.

In the area of access to public information, the Information Commissioner issued 256 decisions in appeal procedures, which are getting increasingly legally complicated. An increase, compared to last year, is seen in the number of appeals relating to the calculation of costs, appeals of the media, and appeals relating to access to the documentation in the public tender procedures. In 2012 the Commissioner also received a much greater number of requests for clarifications, opinions and explanations from applicants and liable bodies. We estimate that the applicants are better acquainted with the institute of access to public information and also use it more often in practice. However, on the other hand with regard to liable authorities we still notice that they are not acquainted with the responsibilities brought by the Access to Public Information Act (also because of the staff and financial shortages). This specifically holds true for bodies of the wider public sector (public institutes, public service contractors, and bearers of public authority, other legal public legal persons). That is why the Information Commissioner held a number of free workshops and presentations for these liable bodies.

With regard to the area of personal data protection for 2012 the Information Commissioner dealt with 725 inspection cases (6% more than in 2011) and 158 offence procedures (16% more than in 2011). In terms of developing trends I would like to draw special attention to cloud computing that is occupying an increasingly important position in terms of data protection and technological development. The potentials of cloud computing are vast, however this should not cause lowering of the level of personal data protection – a fundamental human right. In 2012 the Commissioner published, together with Cloud Security Alliance (CSA) - Slovenia Chapter, ISACA Slovenia Chapter and Eurocloud Slovenia, guidelines for data protection in cloud computing, as one of the first authorities in the EU, to contribute to the establishment of appropriate standards in this field[1]*. The purpose of the document is to establish common control points, by which users as well as supervisory authorities will be able to come to informed decisions regarding the use and oversight of the cloud computing services in part where processing of personal data is concerned. The initiatives for safer use and certifications of cloud services, on the other hand, are offered guidelines for future developments with the goal of compliance with personal data protection legislation. The Information Commissioner finds that many cloud service providers do not yet offer to their prospective clients all the information necessary to make an informed choice. Mechanisms still need to be put in place that will allow for differentiation between the providers that are trustworthy and those that are not.*

Another important trend that must be carefully monitored is the concept of "big data". It refers to vast data bases that are difficult to control with ordinary data base management tools, due to their scope. Such databases allow for quick collection and processing of various (non)structured data sources, making it possible to "see" and "measure" things that were not possible before. With the parallel emergence of "Internet of Things" (e.g. smart phones, devices for future electronic toll collection in cars, smart meters in households consumption, etc..), where the device can collect more and more data in a digital format, the amount of personal data collected experiences an unprecedented increase. The amount of information controlled by the data controller using such technology is so great that it allows for identification of business trends, shopping habits, traffic patterns, all the way to forecasting outbreaks of flu and the likelihood of crime in a given geographical area. As well

[1] https://www.ip-rs.si/index.php?id=308

as the (correct or incorrect) inferences and conclusions about an individual's credit rating, health, shopping habits and other characteristics - data that could not have been inferred previously. Implications for the protection of personal data can be large, that is why "big data" is certainly among the most important new phenomena whose development should be monitored with utmost care, when it comes to question of privacy.

The Commissioner in 2012 devoted considerable attention to preventive action. In addition to the guidelines for the protection of personal data in cloud computing, the Commissioner marked the Data Protection Day and the World Right to Know Day with a variety of activities. The experts from the Information Commissioner shared their knowledge and experiences with colleagues from countries that are still in the phase of establishing an effective system of access to public information and protection of personal data. Among other the Commissioner successfully carried out a twinning light project in data protection in Serbia in 2012. In the context of international cooperation in the field of access to information, the Information Commissioner in 2012 participated in the project LAPSI 1.0, which was completed this year, and joined the project LAPSI 2.0 which will be launched in 2013.

Considering the trends in both areas of the Commissioner's work one would expect more active efforts for effective enforcement of both constitutionally guaranteed rights from the government in the future. In the area of access to public information, I would have liked more efforts to be put in encouraging liable bodies to operate with more transparency which would contribute to greater integrity in the public sector and increase individuals' trust in institutions. Here, again, I cannot pass by the proposal of the necessity of extending the scope of bodies liable under access to public information legislation to the companies where the State, local government or public institutions hold dominant influence. The Minister of Interior and Public Administration promised in April 2013 that our proposals will be taken into account. We will hold him on that promise! In the area of personal data protection I wish for more concern and awareness among data controllers in the public and private sector about the consequences of seemingly trivial, but massive and disproportionate data collection that has brought us into the surveillance society.

The challenges that lie ahead are not at all small and it is important that we face them. The Information Commissioner will continue to perform its work at its best.

However, I wish that everyone would think about what kind of society and state we wish to live in, in terms of privacy and transparency, especially the readers of this report in the National Assembly.

Yours sincerely,

Nataša Pirc Musar,
The Head of Information Commissioner

INTRODUCTION

1 THE INFORMATION COMMISSIONER

1.1 The Establishment and the Competences of the Information Commissioner 1
1.2 Organisational Structure and Budget of the Information Commissioner 3

2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

2.1 Activities in the Field of Access to Public Information in the Republic of Slovenia 5
2.2 The Most Significant Cases and Precedent Cases in Different Areas 7
2.3 General assessment and recommendations in the field of access to public information 11

3 WORK IN THE FIELD OF PERSONAL DATA PROTECTION

3.1 Activities in the field of personal data protection 14
3.2 The Selected Cases Involving a Violation of Personal Data Protection 18
3.3 General Assessment of the Status of Personal Data Protection and Recommendations 20

4 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

4.1 Participation in the Preparation of Laws and other Regulations 25
4.2 Relations with the Public 25
4.3 International Cooperation 26

1 THE INFORMATION COMMISSIONER

1.1 The Establishment and the Competences of the Information Commissioner

On 30 November 2005 the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act[1] (Official Gazette RS, Nos. 113/05 and 51/07 – ZUstS-A, hereinafter: the ICA), by means of which a new and independent state authority was established as of 31 December 2005. The Act combined two authorities, namely the Commissioner for Access to Public Information and the Inspectorate for Personal Data Protection. The Head of the Information Commissioner, who has the position of a state official, is appointed by the National Assembly of the Republic of Slovenia upon the proposal of the President of the Republic of Slovenia. The Head of the Information Commissioner is Nataša Pirc Musar.

In accordance with Article 2 of the ICA, the Information Commissioner is competent to:

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

In the area of access to public information, the Information Commissioner also has the competences determined by the Public Media Act[2] (Article 45, hereinafter: the PMA). A liable authority's refusal of a request by a representative of the media shall be deemed a decision refusing the request. The authority competent to decide on appeals is the Information Commissioner[3].

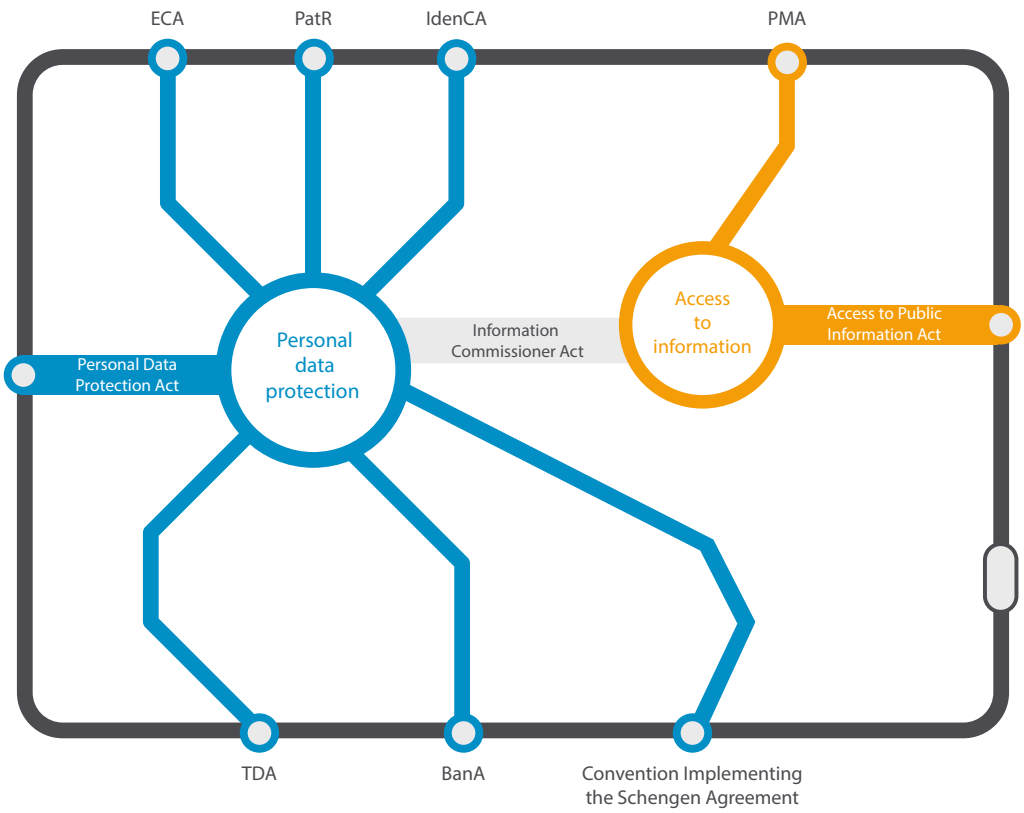
The Information Commissioner also has competences under the Electronic Communications Act[4] (hereinafter: the ECA) which concern the area of inspections of retained traffic and location data acquired or processed in connection with providing public communication networks or services (in accordance with Articles 112 and 147 of the ECA) and in connection with the implementation of European Directive 2002/58/EC on privacy and electronic communications and the Directive on the retention of telecommunications data.

1 Official Gazette RS, No. 113/2005, 51/2007 – ZUstS-A; hereinafter: the ICA.
2 Official Gazette RS, No. 110/2006 – official consolidated text 1, with amendments; hereinafter: the MedA.
3 Official Gazette RS, No. 51/2006 – official consolidated text 2, with amendments; hereinafter: the APIA.
4 Official Gazette RS, No. 13/2007 – official consolidated text 1, with amendments; hereinafter: the ECA.

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

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

Figure 1: Competences of the Information Commissioner.



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

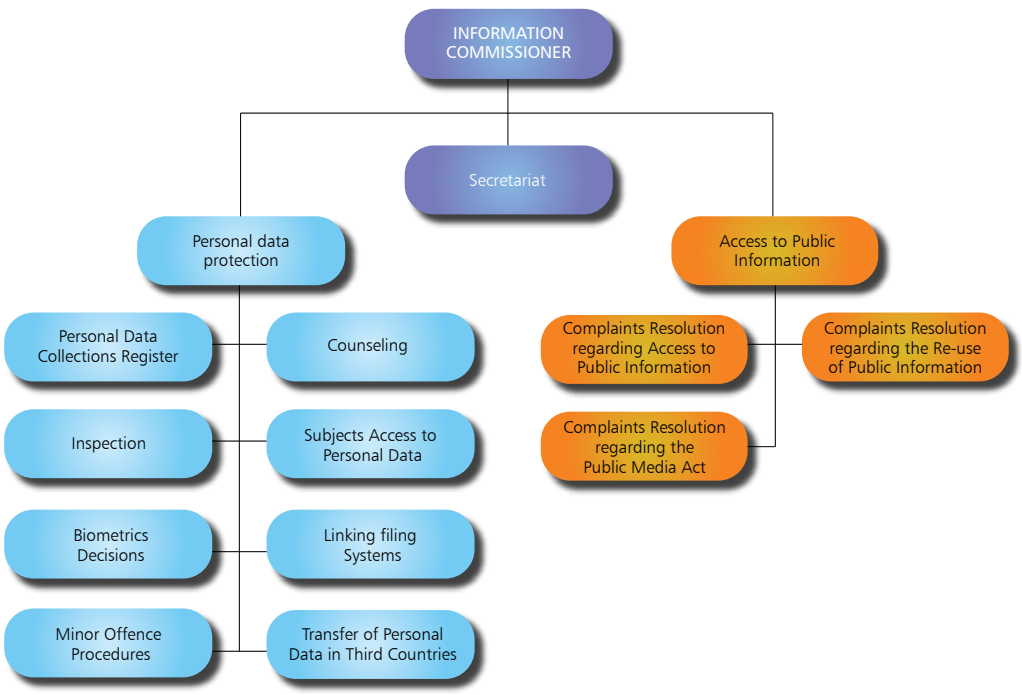
1.2 Organisational Structure and Budget of the Information Commissioner

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

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

At the end of 2012, the Information Commissioner had 33 employees, of which three were employed on the basis of temporary contracts. The number of employees has not changed from 2011.

Figure 2: Organisational Chart of the Information Commissioner.



The work of the Information Commissioner is financed from the state budget; funding is allocated by the National Assembly of the Republic of Slovenia on the proposal of the Information Commissioner (Article 5 of the ICA). In fiscal year 2012, the funding allocated to the Information Commissioner at the start of the year amounted to EUR 1.487.248, 66.

The operational budget at year end amounted to EUR 1.666.574, 20, including European funds for the implementation of projects (LAPSI and Twinning) and the cuts made by the revised budget in June 2012. In 2012 EUR 1.138.678, 08 were spent on wages and salaries. EUR 252.887, 49 was spent on material costs and expenses. Material costs and expenses were necessary for the normal functioning of the Information Commissioner (stationery, travel expenses, cleaning expenses, student work payments, postal services, the education of employees, producing brochures, etc.) A great deal of the expenses stemmed from the rent for our offices.

2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

2.1 Activities in the Field of Access to Public Information in the Republic of Slovenia

The right to access public information was granted by the legislature already in the Constitution of the Republic of Slovenia[9]. The second paragraph of Article 39 of the Constitution determines that everyone has the right to obtain information of a public nature in which they have a well-founded legal interest under law, except in such cases as are provided by law. This right is further regulated in the Access to Public Information Act[10] (hereinafter: the APIA), which ensures everyone free access to and re-use of public information held by state bodies, local government bodies, public agencies, public funds, and other entities under public law, bearers of public authority, and public service contractors. The Act includes the public interest test.

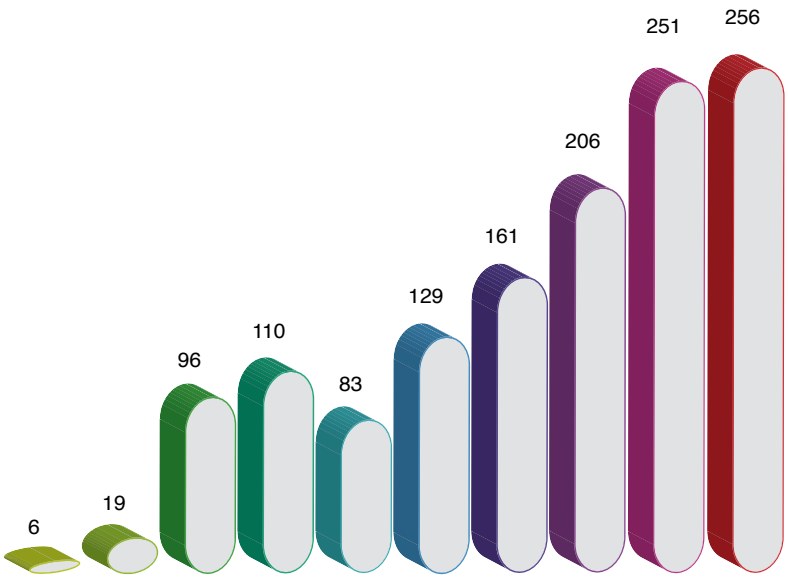
In 2012 the Information Commissioner received 519 appeals, of which 277 were against decisions refusing requests, while 242 were against the non-responsiveness of first-instance authorities. In processing the appeals of individuals, 49 so-called in camera examinations were carried out.

In appeal procedures the Information Commissioner issued 256 decisions, in five cases it rejected the appeal, in 2 cases matters were joined for joint consideration, while 12 applicants withdrew their appeals.

The following actions were taken amongst the decisions issued by the Information Commissioner:

- in 95 cases it dismissed the appeal;
- in 63 cases it granted the appeal of the applicant;
- in 27 cases it returned the matter to the first instance authority for reconsideration;
- in 70 cases it partially granted access to information;
- in 1 cases it rejected the appeal.

Figure 3: The number of decisions issued in relation to access to public information from 2003 to 2012.



[9] Official Gazette RS, Nos. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006; hereinafter: the Constitution.

[10] Official Gazette RS, No. 24/2003 with amendments; hereinafter: the APIA.

In its decisions the Information Commissioner most commonly considered and decided upon the merits of the following:

- whether the documents requested contained personal data whose disclosure would entail a violation of personal data protection in accordance with the PDPA-1 (84 cases);
- whether the liable authority even possesses the document or the public information requested by the applicant (73 cases);
- whether the applicant requested information and/or data deemed to be a business secret in accordance with the Companies Act (61 cases);
- whether a violation of procedural rules occurred (34 cases);

The Information Commissioner decided on an appeal due to access to public information being denied with regard to the following groups of liable authorities:

- public administration (ministries, constituent bodies, public administration units) (97 cases);
- public funds, institutes, agencies, public service contractors, and bearers of public authority (93 cases);
- municipalities (44);
- courts, the State Prosecutor's Office, the State Attorney's Office (19 cases).

In 169 cases applications were submitted by natural persons, in 53 cases complaints were submitted by private sector legal entities. 21 complaints were submitted by journalists and 13 by public sector legal entities.

In 2012 the Information Commissioner received 242 appeals against the non-responsiveness of authorities. The Information Commissioner first called on to the liable authorities to decide on the requests as soon as possible, which in most cases they did. In 25 cases the Information Commissioner rejected the appeal, in 8 cases it issued the explanation that it was not competent to consider their applications and transferred the cases to a competent authority for consideration, and 14 applicants withdrew their appeals.

In 2012, 27 appeals were filed with the Administrative Court against decisions of the Information Commissioner (i.e. against 10,5 % of the decisions issued). The relatively small portion of such appeals, which remains at almost the same level as in previous years, indicates a greater level of transparency and openness in the public sector in relation to its operations and the acceptance of the Information Commissioner's decisions by various authorities and applicants. In 2012, the Administrative Court issued 32 judgments in relation to appeals filed against the decisions of the Information Commissioner. In 12 cases the Court granted the appeals and returned the matters to the Information Commissioner for reconsideration, 16 appeals were dismissed, in 1 case the Court decided partially in favour of the appellants, in 1 case it issued a decision rejecting the appeal, and in 2 cases it issued a decision staying the procedure.

In 2012, the Information Commissioner received 776 requests to provide assistance with regard to various questions of individuals regarding access to public information, especially with regard to the question of whether a certain document contains public information. The Information Commissioner replied to all applications to the extent it is competent, in most instances it referred them to the competent institution – The Ministry of Public Administration.

2.2 The Most Significant Cases and Precedent Cases in Different Areas

Costs of the procedure

By Decision No. 090-272/2011/4 of 6 February 2012, the Information Commissioner annulled the decision of the Administrative Unit Murska Sobota and returned the matter to the body for reconsideration. The applicant requested 51 (operative parts of) denationalization decisions issued during the period of five years. The liable body notified the applicant that the calculated costs of his request amounted to 307, 27 EUR. The applicant did not pay for the costs and the body issued a decision to stay the procedure. The Commissioner pointed out that charging of the cost of work of civil servants in the process of access to public information is an issue, since the law and the Decree on communication and re-use of information of public character do not provide for such charging of costs. However, in deciding on a case the Commissioner must take into account the cost calculation schedule published by the liable body, because it is, as an administrative body, bound by all implementing regulations, and cannot use the institute of exceptio illegalis. Regardless of that the Commissioner found that the charge of EUR 307, 27 for 51 pages is in no way proportionate. For finding and opening of only 51 files the body calculated that 25 working hours were needed, which is clearly disproportionate. Charging of the costs must not be arbitrary, or depending on the individual skills of civil servants or the organization of work at the liable body and the liable body must not transfer the burden of poor organization of work to the applicant. The archives of liable bodies must be organized in accordance with the Decree on administrative operations so that any document sought-after in the archives can be located as soon as possible. The body may also not charge the cost of advisers, which are supposed to monitor, whether the documentation was prepared in order, because the body should not burden the applicant with the costs incurred by distrust of the superiors in the quality of the work of subordinates or to re-verify the quality of the work performed. The Commissioner pointed out that charging of costs of the civil servants' work should not become an opportunity to discourage applicants from submitting applications for access to public information. The costs for providing public information should be at the lowest level that does not interfere disproportionately with the applicant's constitutional right of access to public information.

Re-use of public information

By Decision No. 090-8/2012/2 of 22 February 2012 the Information Commissioner annulled the decision of the Official Gazette of RS and returned the matter of re-use of public information for reconsideration. The applicant requested re-use of public procurement announcements that are freely available on the Public Procurement Portal (www.enarocanje.si). The applicant wished to download the published data on the website and re-use it for commercial purposes: it would gather the information, classify it transparently and enable a search function. Charges would apply to searching. The body supplied to the applicant on a CD all the published data from the beginning of the work of the website and rejected the remainder of the applicant's request. The body also imposed conditions of re-use. In the present case two questions emerged: whether the applicant can require constant updating of the data, and whether it may require the re-use of information that will only be published in the future. The body had asked the applicant to specify the times of re-use and rejected supply of information that has not existed in the time of the request. The Commissioner agreed with the applicant that it may always request for up-to date information. APIA does not specify the request for up-to date information, however this is specifically provided for by the Regulation on the provision and re-use of public sector information. The Commissioner stressed that the essence of the economic function of the re-use of information can only be provided if it enables that the companies acquire up to date, valid and complete information from the public sector, and that the companies do not lag behind the public sector in terms of accuracy of information. Furthermore, the body also requested that the applicant specifies the form in which it wishes to receive

the information, and rejected the request of the applicant to download the information from the website by itself. The Commissioner stressed that APIA does not preclude the acquisition of information directly from the website. Regarding the cost of the provision of information, the Commissioner also noted that APIA provides for charging the costs of re-use of information for commercial purposes, but on the other hand also provides that the liable body cannot charge for re-use of information if it is published on the web free of charge.

Media, personal data

By Decision No. 090-74/2012/4 of 7 May 2012, the Information Commissioner annulled the decision of the Employment Service of Slovenia and requested it to supply the list of the employers who have been issued work permits for supply of work to the citizens of the Dominican Republic for the period the documents are kept, in the way that only the name of the employer and its registration number will be visible. The liable body supplied to the applicant the information about issued work permits for the citizens of the Dominican Republic, for the period the documentation was available and the information of the number of companies that have applied for different permits concerning employment and work. The body did not supply to the applicant the information on the names of the employers and issued work permits at the employees based on the type of work and sex, because disclosure of such data would lead to disclosure of personal data of the individuals employed by a certain company. The applicant appealed in part where access to information on companies that have acquired permits for employees from Dominican Republic was denied. The Commissioner found that all requested information relates to legal persons and is therefore not personal data, and consequently no exception for the protection of personal data is applicable. The company name and registration number are considered public data according to the Companies Act, the Act on the Business Register of Slovenia and the Court Register of Legal Entities Act. The documentation did not involve other exemptions therefore the Commissioner decided that the liable body is to supply the required list.

Internal operations of the body

By Decision No. 090-109/2012/4 of 10 July 2012 the Commissioner annulled the decision of the Municipality of Maribor and ordered it to supply copies of the requested audit report. The applicant requested access to an audit report on the renewal of a given market, labelled as "confidential." The body rejected the applicant's request on the basis of exemption for documentation that is part of internal operations or activities of bodies from point 11 of the first paragraph of Article 6 of APIA. The Commissioner found that the requested report has in fact been made in relation to the internal operations of the body. Internal auditing provides for independent verification of financial management systems (management) and controls and for advice to the management on how to improve their performance. The responsibility for establishing and maintaining an adequate system of financial management, control and internal audit is in the hands of the head of a direct budget user, and internal auditing is performed by internal auditors. Regarding the creation of disturbances in operations or activities of the body, the body claimed that the disclosure of the document would have a negative impact on its business. The Commissioner was satisfied that the body substantiated its arguments, however the body did not advance any reasons why the disclosure of the audit report could led to disruption of the operation, what kind of disturbances it might cause, and what is the level of probability that disturbances might occur. The Commissioner stressed that the disclosure of weaknesses of internal controls of a direct budget user does not automatically mean abuse of those weaknesses and that the body did not prove that disclosure of the document would actually cause disturbances in its operations. With regard to the document being labelled as "confidential", the Commissioner explained that this classification cannot be used in relation to this document, because the content does not relate to public security, defence, foreign affairs or intelligence and security activities as

provided by the Classified Information Act. The exemption on classified information from paragraph 1 of Article 6 of APIA can thus not be applied.

Criminal proceedings, internal operations of the body, personal data, media

By Decision No. 090-196/2012/3 of 4 October 2012, the Information Commissioner partially annulled the decision of the Ministry of Foreign Affairs and ordered supply of reports on the supervision being conducted at the embassy in Paris. The liable body granted to the applicant partial access to the supervision report, in part concerning the premises of embassies and residences and secondary homes, financial and material operations of the Embassy and the records held by the Embassy. Access was granted on the basis of third paragraph of Article 6 of APIA, which provides that access to the requested information is granted when the information is related to the use of public funds or information related to the execution of public functions or employment relationship of the civil servant. The liable body however refused access to those parts of the report, which could, in the opinion of the District Public Prosecutor's Office, prejudice the implementation of a criminal procedure and disrupt internal operations of the body (exemptions from points 6 and 11 of Article 6 of APIA). Regarding the exemption for protection of a criminal proceeding the Commissioner found that the Prosecutor's Office did not substantiate the arguments convincingly and sufficiently. The prosecution stated that disclosure of the information contained in the report would impact the (pre) criminal proceedings where the individuals questioned would not give true and accurate information on the events, but rather their subjective perception of events, mixed up with information from the media. It is supposed to be common knowledge that after a certain time individuals do not recognise the sources where they obtained information anymore. The Commissioner pointed out that the report is not only a set of testimonials and subjective perceptions of individuals who were directly involved in the events and activities at the embassy; it contains objective findings of expert supervision of the Embassy of the Republic of Slovenia in Paris, executed by objective employees of the Ministry of Foreign Affairs. In addition, the report was issued more than three years ago, and even more time has passed since the events in question, that is why the testimonials of the witnesses will lack relevance from time perspective. Much of the information on the specific proceedings is also available to the public, thus it cannot be assumed that disclosure of the report would prejudice the implementation of a criminal procedure. Disclosure of the report as an authentic source might even have benefits for the proceedings. The Commissioner also noted that two telephone numbers appear in the report, which constitute protected personal data, however other personal data are not protected because they refer to the data on the use of public funds or information related to the execution of public functions or employment relationship of the civil servant. The report among other refers to the irregularities in the performance of duties of public servants or officials or other irregularities which occurred at the Embassy in connection to the use of public funds.

Personal data and public interest case

By Decision No. 090-148/2012/8 of 19 October 2012, the Information Commissioner annulled the decision of the Ministry of Internal Affairs and ordered disclosure of a specific part of an opinion and decision of the liable body concerning acquisition of Slovenian citizenship by exceptional naturalization procedure for a specific individual. The body refused access on the basis of the exemption for protection of personal data. The Commissioner established that the documents from the exceptional naturalization procedure contain personal data and meet the criteria for exemption; however the Commissioner also executed a public interest test and held that the public interest in disclosure of the documents outweighs the interests of the specific individual to limit access to the relevant documents. The Commissioner pointed out that the procedure of granting of citizenship by exceptional naturalization is by law conducted because of special state's benefits (interests). It concerns individuals that bring an immense contribution to

the social, economic, scientific, cultural or other development of the Republic of Slovenia or contribute to its international reputation and visibility. The Commissioner determined that the work of such persons in various spheres of social life (rather than private) in the Republic of Slovenia is so important, that their right to protection of personal data, in so far as it relates to the exceptional naturalization, is overridden by the public interest. In this specific case, a prohibition of disclosure of such personal data would prevent public scrutiny over such a sensitive institute such as the institute of exceptional naturalization, which should be used by the executive authorities restrictively and with a high degree of deliberation. The Commissioner also explained that the public interest does not override the protection of personal data that are not directly related to the institute of exceptional naturalization, such as the data on current nationality, date and place of birth and the address of residence.

Public procurement, business secret and public interest test

By Decision No. 090-190/2012/14 of 30 October 2012, the Information Commissioner partially annulled the decision of the Municipality of Maribor and ordered it to disclose to the applicant a considerable part of the contract with Iskra Sistemi d. d. regarding implementation of a radar system. A journalist requested access to the public procurement offer and a copy of the contract of the public-private partnership "Upgrading and automation of road traffic in the Municipality of Maribor" between the Municipality of Maribor and Iskra Sistemi d. d. The body rejected the application in its entirety by reference to the exemption on business secrets. The Commissioner found, firstly, that the conditions for the existence of a business secret by the subjective criterion from paragraph 1 Article 39 of the Companies Act exist. However, the contract and the offer also contained some information that has already been made public by law and, therefore, under the provisions of the Companies Act cannot constitute a business secret. The Commissioner pointed out that anyone who wishes to enter into a contract with a public body, must submit to the specificities of concluding legal transactions (especially to transparency), and cannot expect absolute protection of their data. The Public Procurement Act also provides for disclosure of data, and stipulates that regardless of the data protection certain data included in public procurement (e.g. unit price, the value of individual items, and the total value of the offer, and in the case of the most economically advantageous tender criteria, those data which influenced the ranking of offers in the context of other criteria) are public. Accordingly, the information which shows that the partner meets the terms of the tender and has offered the most economically advantageous solution does not constitute business secrets. APIA in third paragraph of Article 6 also provides that, notwithstanding any exemptions, access must be granted to the information on the use of public funds. Even though the liable body has not paid the private partner any funds directly from the city budget, the contract shows that the partner will receive payment from public funds - from the recovered fines. The Commissioner also noted that business secret cannot apply to the information that has already been known to a wider circle of people, for example, discussed at a public meeting of the City Council and freely available on the World Wide Web (information contained in the proposal of the Act on Public-Private Partnership and Legal Studies on implementation of the partnership). Regarding the rest of the information where the law does not stipulate publicity the Commissioner found that they should be disclosed on the basis of overriding public interest. Establishment of a public-private partnership for a radar system has raised many dilemmas in the local community and wider in Slovenia, being discussed by official institutions, the media and the wider public. Beside the issues of transparency and cost-effectiveness of public spending, the controversies of rights and obligations that a public-private partnership will deliver to individuals were debated. The Commissioner stressed that the individuals participating in the traffic have the right to full and complete information relating to the speeding control of traffic; referring mainly to information about what kind of automated devices are used to monitor the individual, how the system works, what are the obligations regarding maintenance of the information system, which data are collected, and who can access/process them, what are the obligations of the private partner, namely what rights have been transferred to it by the municipality as the public partner. Also in the

public interest is the question of what responsibility was taken over by the municipality and what powers it has delegated to the subject of the private law in such an important area as management and road traffic safety. The Commissioner held that the public interest in disclosure of the documentation relating to such information prevails; access to the rest of information may be rejected based on business secret exemption.

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

The Information Commissioner can assess the year 2012 as positive in terms of access to public information. In 2012 it received 1295 cases to handle, which is less than the year before. The number of complaints has decreased mainly on account of significantly fewer complaints against the non-responsiveness of the first-instance bodies. In 2012 it handled 242 such cases, whereas in 2011 it handled 549 such cases. After several years of increasing numbers of complaints against non-responsive bodies, 2012 is the first that shows a decrease, indicating a greater responsiveness of the first instance bodies. At the same time, the number of questions, requests and initiatives for clarifications regarding the use of APIA in practice increased (a total of 776 cases in 2012, and 699 cases in 2011), and the number of complaints against decisions refusing access remained at a comparable level.

Based on the above information and executed appeal procedures the Information Commissioner believes that the applicants and the liable bodies are better acquainted with the institute of access to public information; however in practice more activities for promotion of this right and training for the liable bodies will be needed. This is reflected by the number of questions and requests for clarifications regarding the application of the law in practice, which increased in 2012. In particular, municipalities and authorities of the wider public sector (public institutions in the area of education, health, and other legal persons governed by public law) and public service and public authorities, who are legal persons governed by private law, are still poorly informed about the obligations imposed on them by APIA. In this regard the Information Commissioner calls on the competent ministry (currently the Ministry of Justice and Public Administration), to take on a more active role in this area. Promotional and developmental tasks, as well as advice to the liable bodies about APIA are the task of the competent ministry. The Information Commissioner can provide unofficial advice to liable authorities, however, as the appellate authority it is not allowed to take sides in advance with regard to specific cases.

It should also be noted that the liable bodies as the first instance bodies as well as the Information Commissioner as the appellate body are faced with increasingly complex cases every year. In 2012, a significant increase can be noted in the number of cases relating to access to documents in public procurement procedures. These procedures include deciding on vast documentation scope, inclusion of secondary participants and consideration of multiple exemptions (business secrets, personal data). Similarly an increase is noted in cases where the applicants are journalists under Article 45 of the Media Act, where the short deadline for a decision is crucial. The Information Commissioner finds that the appeal proceedings are often the result of procedural errors made by the first instance body (by the non-inclusion of secondary participants, the lack of timely response to requests) and unfamiliarity with the legal provisions of the law and in implementation of the law in practice, which can be resolved through regular and mandatory training of access to public information officers from the liable bodies.

As in the previous years, the Information Commissioner would again like to call attention to the charging of fees for the work of public officials related to accessing information. In 2012 an increase can again be observed in the number of complaints with regard to charging

of the costs. What is worrying is the fact that liable bodies have charged fees even for simple access to documentation, even though Article 43 of APIA clearly states that access to documentation must be free of charge. Additionally, the Decree on Communication and Re-use of Information of Public Character has not been amended yet. On the basis of the Decree the liable bodies are able to charge the applicants completely arbitrary for the cost of work of civil servants in relation to the APIA request. The Commissioner has been highlighting this inconsistency between the Decree and APIA since 2009.

In 2012, the Information Commissioner repeatedly exposed publicly the need for widening the scope of the bodies liable under access to public information legislation, to include the companies where the State, local government or public institutions hold dominant influence. The practice has showed that those are the entities whose business is directly or indirectly in the public interest and the public does not have access to any information about their operations on the basis of the current APIA because they are subjects of private law.

In 2012 the Information Commissioner received two appeals from the field of the reuse of public information, which indicates applicants' poor knowledge of the legal mechanisms available to them if their request is not granted. The reuse of public information has important economic potential which remains underexploited in practice. This has also been pointed out by the European Commission, which was facilitating public discussion on the draft amendments to the Directive of the European Parliament and Council of 17. 2. 2013 on the Reuse of Public Sector Information. The purpose of it is to ensure an optimal legal framework and changes in the public sector culture in order to foster the digital content market for products and services that are based on public sector information and to prevent distortions regarding competition in the market. The amendments are to contribute to creation of new employments as well. In the field of the reuse of public information, the Information Commissioner in 2012 again actively participated in the international consortium within the LAPSI project (Legal Aspects of Public Sector Information), which is intended to establish a thematic network in the field of the reuse of public information.

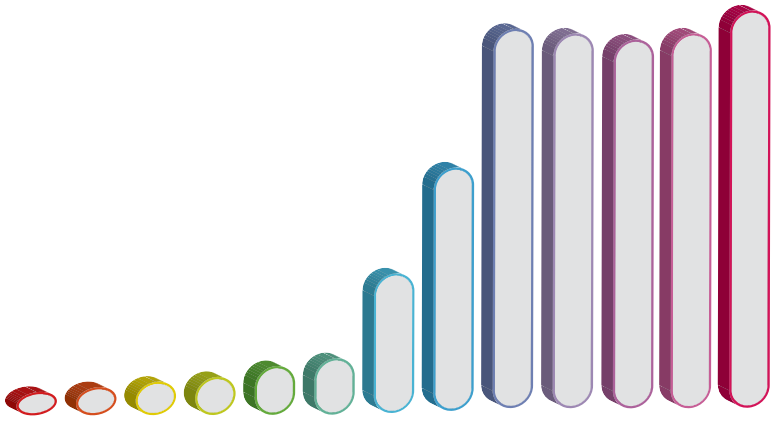
3 WORK IN THE FIELD OF PERSONAL DATA PROTECTION

3.1 Activities in the field of personal data protection

In the Republic of Slovenia the concept of personal data protection is based on the provisions determined by Article 38 of the Constitution, according to which personal data protection is among the constitutionally guaranteed human rights and fundamental freedoms. The PDPA is an organic law that has been valid since 1 January 2005, while the amended PDPA-1[11] was adopted in July 2007. The purpose of organic laws is to define in a uniform manner general rights, obligations, principles, and measures by means of which unconstitutional, illegal, and unjustified interferences with the privacy and dignity of individuals in the processing of personal data are prevented. Therefore, sectoral laws must clearly determine which filing systems will be established and maintained with regard to individual fields, the types of personal data that individual filing systems will contain, the manner of personal data collection, the possible limitations of the rights of individuals, and, above all, the purpose of processing the collected personal data. With regard to Part VI, the PDPA-1 is also a so-called sectoral law which by means of the exact definition of rights, obligations, principles, and measures provides data controllers with a direct legal basis for personal data processing in the field of direct marketing, video surveillance, biometrics, recording the times of persons entering and exiting buildings, as well as professional supervision. Furthermore, what is also used in Slovenia are the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Convention was ratified in 1994[12].

Due to the suspicion of violations of the provisions of the PDPA-1, in 2012 the Information Commissioner conducted 725 cases of inspection, of which 245 pertained to the public sector and 480 to the private sector. It received 237 complaints against public sector legal entities, on the basis of which it initiated 212 inspection procedures, while it initiated 33 procedures ex officio; furthermore, it received 510 complaints against the private sector and upon such basis initiated 446 procedures, while it initiated 34 procedures ex officio. The number of complaints and appeals due to the suspicion of violations of the PDPA-1 increased in comparison to the statistical data for 2011. Within the framework of inspection procedures, 62 physical inspections were carried out in the public sector and 115 in the private sector. In order to redress the established irregularities, in 2012, 18 warnings were entered into the records and 74 regulatory or administrative decisions were issued. In 2012, 233 decisions to stay procedures were issued.

Figure 4: The number of cases that the Information Commissioner conducted on the basis of suspected violations of PDPA-1 provisions between 2000 and 2012.

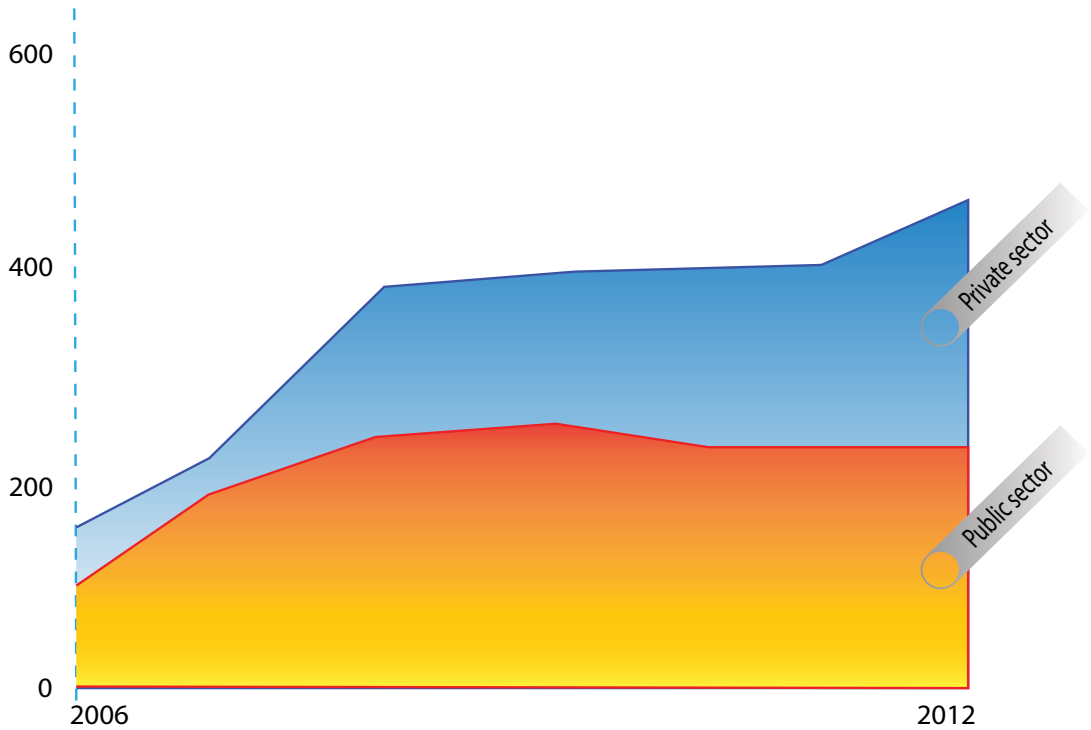


[11] Official Gazette RS, No. 86/2004; hereinafter: the PDPA-1.
[12] Official Gazette RS, No. 11/1994 – International contracts no. 3/1994.

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

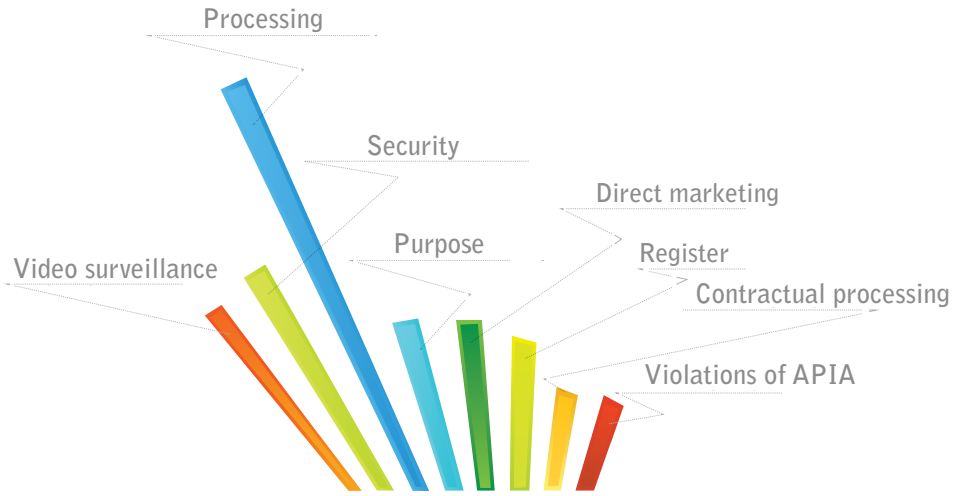
- unlawful disclosure of personal data; the transfer of personal data to unauthorised users by data controllers and unlawful publication of personal data (226 cases);
- unlawfully collecting or requiring personal data (144 cases);
- abuse of personal data for direct marketing purposes (119 cases);
- unlawful video surveillance (72 cases);
- inadequate security of personal data (44 cases);
- other (120 cases).

Figure 5: Complaints regarding unlawful processing of personal data from 2006 to 2012, a comparison between the public and the private sectors.



In 2012, 158 offence procedures were initiated due to PDPA-1 violations, of which 29 were against public sector legal entities, 78 against private sector legal entities, and 51 against individuals. In offence procedures in 2012 the Information Commissioner issued 17 warnings, 119 decisions regarding violations (61 cautions and 51 fines), and 7 penalty notices. Furthermore, the Information Commissioner issued 87 warnings for minor violations. Violators filed 30 requests for judicial protection against the decisions issued. In 2012 competent authorities stayed procedures in 6 cases by means of an official note stating that there was not sufficient evidence to pronounce sanctions or since it was found that the action alleged was not a violation.

Figure 6: The most common violations of PDPA-1 provisions in 2012.



In 2012, the Information Commissioner received 17 judgments whereby local courts decided on requests submitted for judicial protection against decisions by the Information Commissioner regarding offences. The decision of the Information Commissioner was upheld in 10 cases, the sanction for the offender was changed in 4 cases, and the decision of the Information Commissioner was annulled in 3 cases.

In 2012, the Information Commissioner received 2.191 requests to issue a written explanation or an opinion in relation to specific questions. It issued 143 written opinions and explanations, and in 2.048 cases it referred applicants to opinions and explanations already issued. It also issued 62 opinions to requests received from abroad. Most opinions are published on the following website: www.ip-rs.si. Furthermore, the Information Commissioner issued opinions and explanations orally. Every working day between 9 a.m. and 3.30 p.m. there is an officer on duty at the office who can answer questions over the telephone.

In 2012, 7 decisions were issued on the permissibility of implementing biometric measures. The Information Commissioner granted the request of the applicant who will, by means of biometric measures, protect a server room where business secrets and personal data are stored; the request of an applicant who will secure a number of spaces where it handles precious metals of great value; the request of a bank which wished to secure business secrets by implementing biometric measures at the entrance of the chairman's office; an applicant who wanted to secure the so-called clean premises of laboratories in which cell products are developed and stored; an applicant who wanted to secure the premises of a telecommunication area where assets of great value are located. The Information Commissioner rejected the request of an applicant who wanted to use biometric measures to secure the premises of a kindergarten, by at the same time registering the working hours of employees, and of an applicant who wanted to protect access to its premises and use biometric measures for the registration of the working hours of employees.

In 2012, the Information Commissioner received five applications for the transfer of personal data out of the Republic of Slovenia. It issued five decisions and permitted the applicants to transfer personal data: to two companies which will transfer personal data of employees to India for the purpose of human resources management, a pharmaceutical company that will transfer the data of employees to a contractual partner in India for IT reasons, a company that will transfer personal data of employees and business partners to India for accounting purposes. The Commissioner also decided that the Republic of Macedonia ensures an adequate level of personal data protection.

In 2012, the Information Commissioner permitted 12 data controllers to link with another or other personal data filing systems. It permitted the linking of filing systems to the following institutions: the Health Insurance Institute of Slovenia and Ministry of Education, Science, Culture and Sport (the Register on insured persons – mandatory insurance and the Information system of the higher education of Slovenia); the Ministry of Labour, Family, and Social Affairs and Ministry of Higher Education, Science and Technology (Central register of rights acquired from public funds and Information system of the higher education of Slovenia), the Ministry of Labour, Family, and Social Affairs and Ministry of Education and Sport (Central register of rights acquired from public funds and Central register of the participants to education and schooling); Ministry of Finance and Customs Administration (Resister on tax foreclosure and Tax register); Ministry of Higher Education, Science and Technology and Ministry of Internal Affairs (Information system of the higher education of Slovenia and Central population register); Ministry of Education, Science, Culture and Sport, and Higher Education Institutions (the Information system of the higher education of Slovenia and filing systems kept by the Institutions); State Attorney`s Office and Ministry of Internal Affairs (Register of registered cases and Central population register); Supreme Court of the Republic of Slovenia and the Ministry of Internal Affairs (the Registry of penal procedures and the Central population register); State Prosecutor`s Office and Ministry of Internal Affairs (the Register of the State Prosecutor's Office and the Central population register); Ministry of Labour, Family, and Social Affairs and Supreme Court of the Republic of Slovenia (Central register of rights acquired from public funds and E-land register), Health Insurance Institute of Slovenia and Agency of the Republic of Slovenia for Public Legal Records and Related Services (the Register on insured persons – mandatory insurance and Slovenian Business Register); Health Insurance Institute of Slovenia and Ministry of Education, Science, Culture and Sport (the Register on insured persons – mandatory insurance and Central register of the participants to education and schooling), General Hospital of Jesenice and Ministry of Internal Affairs (e-births).

In 2012, the Information Commissioner received 63 appeals regarding the right to access to one's personal data, which is less than in the previous year (85). The appeals filed concerned state authorities, ministries, and constituent bodies (21 cases), health care institutions (12 cases), insurance companies (4 cases), telecommunications operators (3 cases), banks (2 cases), courts (2 cases), municipalities (1 case) and other data controllers such as associations (15 cases). In 19 cases data controllers enabled individuals access to requested data upon being called on to do so, while 14 data controllers were ordered by a decision to do so. Three applicants were advised how to act, while two withdrew their appeals. The Information Commissioner transferred 13 appeals to competent authorities for consideration, in 16 cases it issued a decision rejecting the appeal on the grounds that the application was incomplete or had been submitted prematurely, and in 1 case it issued a decision dismissing the appeal.

In 2012, the Information Commissioner filed two requests for a review of the constitutionality to the Constitutional Court of the RS. The first concerned constitutionality of an article in the Prevention of Restriction of Competition Act[13] which provides the competition authority with the competency to review business records and correspondence regarding the operations of the company, regardless of the media where it is kept. It also provides that the company must allow the review of documentation and access to premises, and that the authority may conduct an investigation against the will of the company. Such a provision is in the Commissioner's opinion not in line with Article 37 of the Constitution of the RS, which provides that each individual has the right to privacy of his communication and correspondence. The business communications made by e-mail are made by individual employees and can constitute their private correspondence as well, hence the competencies of the competition authority to review e-mail communications of employees can breach Article 37 of the Constitution of the RS. The second request concerned constitutionality of an article in the Ordinance on road traffic regime in the Municipality of Ljubljana, which provides that public roads and other public surfaces may be subject to video surveillance

[13] Official Gazette RS, No. 36/2008 with amendments; hereinafter: the PRCA.

for the purpose of monitoring road traffic, enforcement of road traffic legislation, better management of the traffic system and traffic security. The Municipality of Ljubljana was to be the controller of such collected data. The Commissioner argued that any data processing must be provided for by the law, and not a lower level legal act, and that processing of personal data of individuals does not fall among the original tasks and competencies of municipalities. Furthermore, a breach of privacy in such case is not proportionate considering the goals of managing the traffic system that could have been achieved by milder means.

In 2011, the Information Commissioner filed a request for a review of the constitutionality of the two articles of the Real-Estate Recording Act[14]. In 2012 the Constitutional Court of the RS ruled that the two articles which determine the public nature of the name, family name, permanent residency address, and the year of birth of individuals entered in the cadastre of buildings and the land cadastre are not in line with the Constitution of the RS. The two articles were repealed.

3.2 The Selected Cases Involving a Violation of Personal Data Protection

Data on employees' printing

The Information Commissioner received a complaint that the management of a state authority requested a list of all employees and their use of work printers (names, surnames, the number of prints, titles of documents). In the inspection procedure it has been established that the authority needed to monitor the costs of printing and therefore used an application to establish that the employees were actually making irrational and non-ecological use of printing facilities, printing also their personal matters. The Commissioner concluded that the authority should not have been collecting the data on the title of the document or the printed website, as these are personal data that are not necessary to effectively manage the processes and cost of printing that needs to be done by the authority. The Commissioner ordered that the said data must not be collected further and that the application be adapted, however, the authority decided not to use the application anymore.

Collection of data for direct marketing online

The Information Commissioner received a number of complaints regarding a data controller performing direct marketing via e-mail, allegedly without the individual's consent to processing of their personal data. In the inspection procedure it has been established that the data controller held in its data bases data on more than 100.000 individuals, registered users of its website and users of certain Facebook applications. The Commissioner concluded that the data controller presented sufficient evidence that it obtained consent from the registered users of its website, however did not present sufficient evidence with regard to Facebook application users, who have allegedly consented by installing different applications. When a user installs a Facebook application the controller's servers should have by default recorded some background data such as the time of installation or IP address or similar. Since the controller did not present any evidence but instead claimed that the sole existence of the data in its data bases testified that the users have consented, the Commissioner ordered for the data to be deleted. The data controller implemented the order.

[14] Official Gazette RS, No. 47/2006 with amendments; hereinafter: the ReRA.

Biometric measures in a fitness studio

The Information Commissioner received a complaint that a fitness studio performs biometric control over its customers who wish to enter the premises, and has video surveillance cameras installed in locker rooms. In the inspection procedure it has been established that the fitness studio actually performed biometric checking of the customers entering the premises, however the customers were able to choose between a key card with a chip and no biometric data, and biometric checking, which included a template of the customers fingerprint. The controller did not store the customers' fingerprints but only the templates and believed that such activity does not fall under the regime of biometric data processing. The Commissioner clarified that such storing of templates constitutes processing of biometric data. It ordered the fitness studio to stop processing biometric data because it did not have a legal basis for such processing. The PDPA-1 only allows, under certain conditions, implementation of biometric measures over the employees and not customers. It has also been established that the fitness studio performs video surveillance in locker rooms, where this is forbidden by law. The Commissioner ordered the studio to either stop video surveillance of the locker rooms or ensure the customers have other rooms available where they can change clothes without being monitored.

The visitors of a gambling website redirected to another web address

The Commissioner initiated a procedure against the Office for Gaming Supervision which registered a domain to which all visitors of gaming sites that operate without the government's concession were redirected. In the inspection procedure it has been established that the data controller does not have a legal basis in the law to collect and process the information on the visitors of the gaming sites that operate without the government's concession. The Gaming Act[15] provides that access to such websites may be limited but does not provide for any processing of the data of the visitors in such a way that visitors are redirected to the controller's website and their data (such as IP address, time of visit, browser details, etc.) are processed by the controller in such a way. The Information Commissioner held that IP addresses are personal data as well as the data on browser details which provide for a unique fingerprint of the visitor. The Commissioner ordered the controller to delete from its data bases the data that could uniquely identify the visitors and not to collect those data in the future. The Controller executed the order and filed an appeal to the Administrative Court against the Commissioner's decision. The Court has not decided yet on the merits of the case.

Processing of personal data in bicycle renting service BicikeLJ

The Information Commissioner received a number of complaints regarding a new bicycle renting service BicikeLJ where the data controller requested a number of personal details of the users who wished to register for the service, including such that were not necessary in relation to the service. In the inspection procedure it has been established that the data controller collects and processes different personal data based on the type of service a user wishes and on the type of payment (credit card or direct debit). The legal basis is the contract between the user and the service provider. It has been established that in none of the cases the data controller can show that it requires for the fulfilment of the contract the data on the gender, and mobile phone number of the users. Additionally, for the users that pay for the service with a credit card the data controller should not require the home address of the users. The Commissioner established that the said data may be collected and processed based on user consent, however such consent must be freely given and the user must be presented with a choice whether it wishes to supply the data to the service provider, as those data are not necessary for the fulfilment of the bike renting contract. The data controller executed the order and filed an appeal to the Administrative Court against the Commissioner's decision.

[15] Official Gazette RS, No. 27/1995 with amendments.

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

Like in the previous years in 2012 the highest number of complaints received by the Information Commissioner concerned unlawful disclosure of personal data; the transfer of personal data to unauthorised users by data controllers and unlawful publication of personal data on the internet or in the media, followed by unlawful collecting or requiring personal data, abuse of personal data for direct marketing purposes, and unlawful video surveillance.

In 2012 the Information Commissioner conducted 725 cases of inspection in the field of data protection, of which 245 pertained to the public sector and 480 to the private sector (in 2011 it handled 682 cases, and in 2010 599 cases). In 2012, 158 offence procedures were initiated due to PDPA-1 violations (136 in 2011 and 179 in 2010). The statistics show that the number of inspections is still gradually rising, however it needs to be noted that in many cases after the inspection procedure has been initiated it has been established that there had not been a violation and that the complaint was filed by the applicant with the desire to intentionally interfere with the legal or natural person's interests or as a revenge.

Aside from inspections and offence procedures, in 2012, the Information Commissioner received 2.191 requests to issue a written explanation or an opinion in relation to specific questions (2.143 in 2011 and 1.859 in 2010), 9 requests for a decision on the permissibility of implementing biometric measures (9 in 2011 and 6 in 2010), 5 requests for authorisation of a transfer of personal data to third countries (4 in 2011 and 8 in 2010), and 63 appeals regarding the right to access one's personal data (85 in 2011 and 85 in 2010). It follows from the statistics that there is no noticeable decrease in the number of these requests compared to the previous years.

Among cases related to direct marketing, complaints regarding direct marketing via e-mail prevail, where marketers often cannot demonstrate in what manner they obtained e-mail addresses, which suggests that they obtained such in an unlawful manner. It is worth noting here a large number of group buying websites providers, which have recently emerged in the market, and very often could not show they have obtained consent of the individual whose e-mail addresses they have processed. Here it is again necessary to stress that many marketers did not stop sending unwanted e-mail messages even after individuals have requested such. In such cases the Commissioner initiated an offence procedure and fined the marketers according to Article 94 of PDPA-1.

In the past the Commissioner regularly called upon data controllers to take account of the necessity of security of personal data collected over the internet or being used for direct marketing via e-mail, and had fined them for disrespect of these rules. However, the number of such cases has not decreased. In last year there has still been a number of cases regarding unlawful disclosure of the e-mail addresses of the recipients of a message in the "To" or "Cc" fields when such addresses should have been entered in the "Bcc" field, such as when notifying applicants about a vacant work place. There were also cases where data controllers did not ensure measures of security such that it was possible, without authorisation and only with the use of search engines, to obtain personal data stored and processed by websites.

With the implementation of the Exercise of Rights to Public Funds Act[16] the Information Commissioner started to receive complaints regarding Social Work Centres that decide upon the rights. The reason for complaints was that the Social Work Centres in decisions disclosed the data on income and property of all the parties that were considered to reach such a decision. In most of the cases the Commissioner established that such disclosure

[16] Official Gazzente no. 62/2010 with ammendments; hereinafter ERPFA.

does not amount to a breach of the law because it relates to collection and processing of personal data that is necessary to reach a decision on the rights to public funds of an individual, where it is necessary to include in a decision the type and level of income, and the value of the property of all the persons whose income and property were considered in reaching a decision. Unlawful collection and presentation of personal data in decisions was only established in cases of persons whose income and property should not have been considered in decisions regarding the material status of the applicant, according to Article 11 of the ERPFA.

In terms of developing trends cloud computing is occupying an increasingly important position. The potentials of cloud computing are vast, however this should not cause lowering of the level of personal data protection – a fundamental human right. This is also one of recommendations of the International Working Group for Data Protection in Telecommunications (IWGDPT) in the "Sopot Memorandum on data protection in cloud computing[17]. The Information Commissioner gave an important contribution to the memorandum that shows consensus between data protection authorities worldwide, and has been also active on national level.

In 2012 the Commissioner published, together with Cloud Security Alliance (CSA) - Slovenia Chapter, ISACA Slovenia Chapter and Eurocloud Slovenia, guidelines for data protection in cloud computing, as one of the first authorities in the EU, to contribute to the establishment of appropriate standards in this field[18]. The purpose of the document is to establish common control points, by which users, as well as supervisory authorities, will be able to come to informed decisions regarding the use and oversight of the cloud computing services in part where processing of personal data is concerned. The initiatives for safer use and certifications of cloud services, on the other hand, are offered guidelines for future developments with the goal of compliance with personal data protection legislation. The Information Commissioner finds that many cloud service providers do not yet offer to their prospective clients all the information necessary to make an informed choice. Mechanisms still need to be put in place that will allow for differentiation between the providers that are trustworthy and those that are not. In times when many activities in the fields of standardisation, certification and other mechanisms for building trust in cloud computing are taking place, we hope, that these guidelines will offer some much needed help in decision making processes to any organisation, small or big, that is considering to use one of the many cloud services on the market, such as office packs, customer relationship management systems, e-mail servers and other business applications, infrastructure and platforms.

Another important trend that will play an increasingly important role is the concept of "big data". In simple terms it refers to vast data bases that are difficult to control with ordinary data base management tools, due to their scope. Such databases allow for quick collection and processing of various (non)structured data sources, making it possible to "see" and "measure" things that were not possible before. With the parallel emergence of "Internet of Things" (e.g. smart phones, devices for future electronic toll collection in cars, smart meters in households consumption, etc..), where the device can collect more and more data in a digital format, the amount of personal data collected on individuals experiences an unprecedented increase. Imagine for example the quantity of data being processed by Facebook, Amazon or Google (Wal-Mart for example processes a million of transactions per second) and what this data might reveal. The amount of information controlled by the data controller using such technology is so great that it allows for identification of business trends, shopping habits, traffic patterns, all the way to forecasting outbreaks of flu and the likelihood of crime in a given geographical area. As well as the (correct or incorrect)

[17] IWGDPT: Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April. 2012, Sopot (Poland): http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

[18] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

inferences and conclusions about an individual's credit rating, health, shopping habits and other characteristics - data that could not have been inferred previously. Implications for the protection of personal data can be large, that is why "big data" is certainly among the most important new phenomena whose development should be monitored with utmost care, when it comes to question of privacy.

The Information Commissioner has been devoting attention to the field of electronic communications development and, similarly to last year, calls attention to the fact that increased tendencies for surveillance of e-communications are emerging and raising conflicts between different interests and rights.

In the 2011 annual report the Commissioner highlighted the inappropriate provisions of the Gaming Act that provides that access to certain gambling websites may be limited/blocked by the internet service providers and attempts to widen the competencies of the supervisory bodies regarding the use of the data retained in line with the general data retention provisions. The Government proposed changes to Article 149b of the Criminal Procedure Act that would enable obtaining not only data related to specific telephone numbers but data related to an entire mobile telephony base station. The worrisome trend continued in 2012, in the process of amendments to the Electronic Communications Act, where the Information Commissioner invested a lot of efforts into proposing amendments, however some of the good proposals and some controversial ones have been overlooked due to the process of proposing amendments. The law enforcement has once again attempted to simplify the regime of their access to the data on identification of the persons communicating electronically. The proposed Article 166 provided that in order to obtain the information on identification of an individual, law enforcement must present a written request from the competent body, and not a court order, as was provided by the Act before amendments, compliant with Article 37 of the Constitution of the RS which provides that the privacy of correspondence and other means of communication shall be guaranteed. Only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security. The Constitution therefore foresees strict conditions under which communication privacy may be invaded, namely a court order. Obviously the suggested amendments were another attempt of avoidance of the Constitution. The Information Commissioner invested many efforts, press releases and public appearances, to achieve that the proposed amendments received a public critique and was in the end removed from the proposal. Regardless of the success we need to stress that such actions have become symptomatic and persistent attempts of the law enforcement to lower the level of communication and information privacy with unconvincing arguments and different laws to make communication data more easily accessible for them. Ever more often is is clear that the traffic data, e. g. who communicated when to whom, are more important than the content of the communication. Both are protected categories according to Slovenian Constitution.

The Information Commissioner as well finds that the police are increasingly trying to widen its competencies, without substantiating its arguments with analyses that would clearly show that additional competencies are:

- necessary (it is not possible to limit crime with milder measures),
- efficient (the technical means actually enable the goal to be reached),
- proportionate as regards invasion of human rights (the goal cannot be reached with a milder measures, such as with ordinary police work).

Such analyses (Impact Assessments) should have been performed before new competencies are introduced or amendments to acts proposed such that in essence increase the risks for violation of personal data protection. The necessity and efficiency of the measures would have to be re-assessed on a regular basis even later (Regulatory Impact Assessment). Unfortunately, regarding the two proposals, none of the suggested analyses was made, on contrary, there have only been short arguments unsubstantiated with statistics and data.

In 2012, the Information Commissioner continued its preventative activities and privacy impact assessments. It provided its prior assessment and opinion with regard to various projects, from the public and private sector, with the goal of identification and management of privacy risks. The projects included the use of smart boards and RFID chips in an ER, the use of GPS devices to monitor the delivery, internal e-elections in an organization, the use of cloud services, Implementation of Registry of the Higher Education, the use of city card Urbana in libraries, online DNA analysis, amendments to general acts of information security, tracking users with screen capture technology, smart meters in households, implementation of central monitoring after quality control, credit score systems, encryption of data in electronic networks, linking of registries of detained persons, archiving e-mails, and the use of cookies.

4 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

4.1 Participation in the Preparation of Laws and other Regulations

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

In 2012, the Information Commissioner participated in the preparation of 53 acts and other regulations, including the following:

- the proposal of a General Data Protection Regulation (opinion of 27 February 2012);
- the Draft Act Amending Road Transport Act (opinion of 24 May 2012);
- the Draft Act Amending Electronic Communications Act (opinion of 22 September 2012);
- the Draft Act Amending Tax Procedure Act (opinion of 16 July 2012);
- the Draft Act Amending Act on Police Tasks and Authorities (opinion of 3 September 2012);
- the Draft Act Amending Act on Public Procurement (opinion of 29 October 2012);
- the Draft Act Amending the Gaming Act (opinion of 4 November 2012).

4.2 Relations with the Public

Throughout 2012 the Information Commissioner provided for the public nature of its work through its website www.ip-rs.si and it raised the awareness of legal entities and natural persons by means of regular and consistent contact with the media (by means of press releases, statements, commentaries, interviews with the Head of the Information Commissioner, press conferences). It endeavoured to ensure that its website was up to date and comprehensive. The majority of information on its website is also available in English. By organising a variety of workshops and seminars it provided for the continuing education of liable entities and persons; furthermore, it participated in a number of conferences, workshops, and round tables. The Commissioner also communicates via social media, through its Facebook profile.

In 2012 the Information Commissioner continued its preventative work and dedicated a great deal of attention to continuing to disseminate tools and aids for raising awareness. It issued Guidelines of data protection in cloud computing and Guidelines regarding data transfer to third countries. The Commissioner takes an active role in the Centre for Safer Internet of Slovenia, whose mandate is to create a safe and open internet environment for children.

On 28 January 2012 the Information Commissioner marked European Personal Data Protection Day and prepared an event intended to draw attention to the importance of personal data protection in the use of social networking sites, specifically among the youth. It organised a public contest among high schools for the best video on the topic of Data protection and social networking sites. As has become a tradition, on this occasion the Information Commissioner awarded a prize for good practice in the area of personal data protection to two data controllers, one from each the private and the public sectors. In 2012 the special award "Privacy by Design Ambassador" 2011 was awarded for efforts in the field of privacy by design. The award was bestowed upon the company Acros d. o. o. for their project TRACE. Furthermore, awards were given to companies which in 2011 became certified in accordance with the ISO/IEC 27000 information security management standard and thus demonstrated a high level of personal data security.

Every year on 28 September the International Right to Know Day is marked. On this occasion organizations from all over the world emphasise the importance of the fight for transparency and accountability of the public sector and of ensuring efficient participation of citizens. In this regard the Commissioner notes that in Slovenia there are still many bodies that do not react to citizen requests for access to public information. Additionally, the Commissioner stresses the necessity of extending the scope of bodies liable under access to public information legislation to the companies where the State, local government or public institutions hold dominant influence. They operate with public funds or under influence of public administration therefore their accountability to the public should have been higher. This year the Commissioner also issued a brochure Information – an inexhaustible source of business ideas which is to promote the potential of reuse of public data.

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

4.3 International Cooperation

Information Commissioner`s employees regularly participate in international seminars and conferences where they often present their own papers.

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

In 2012, the Information Commissioner actively participated in six EU working bodies engaged in supervision of the implementation of personal data protection within individual areas of the EU, namely the following:

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

In 2012, the Head of the Information Commissioner continued to hold the position of Vice-Chairman of the Europol Joint Supervisory Body. In February 2012 a Deputy Information Commissioner participated in the international inspection group that carried out an inspection regarding personal data protection at Eurojust's headquarters in the Hague. The Information Commissioner also regularly participated in the International Working Group on Data Protection in Telecommunications (IWGDPT). Once again in 2012, a representative of the Information Commissioner participated in the Council of Europe's Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

In 2012, the Information Commissioner hosted representatives of similar institutions from a number of countries, such as Serbia, Georgia, Macedonia and Albania to whom it

presented its activities and good practices in its fields of competence. As a Junior Partner it successfully finished the Twinning project IPA 2009, No. MN/09/IB/JH/03 – "Implementation of Personal Data Protection Strategy" in Montenegro and it started the implementation of the Twinning Light Project SR/2009/IB/JH/01 – "Improvement of Personal Data Protection" which is focused on improving personal data protection in Serbia.

In 2012, the Information Commissioner continued and in September finished its work within the European LAPSI project (Legal Aspects of Public Sector Information), which is intended to establish a thematic network of experts in the field of the reuse of public information in order to remove obstacles to its implementation that occur in practice.

Editor:

Nataša Pirc Musar

Authors:

Monika Benkovič Krašovec, PhD, State Supervisor for the Protection of Personal Data
Jože Bogataj, Head of State Supervisors for the Protection of Personal Data
Alenka Jerše, Secretary General
Eva Kalan, Advisor
Polona Tepina, Advisor
Kristina Kotnik Šumah, Deputy Information Commissioner
Andrej Tomšič, MA, Deputy Information Commissioner

Design:

Klemen Mišič, **Matjaž Drev, MA** in **Bons, d. o. o.**

Photography:

Fotolia and **Klemen Mišič**

Translation:

Jelena Burnik, MSc, Advisor

Address:
Informacijski pooblaščenec RS
Zaloška cesta 59
1000 Ljubljana

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

Ljubljana, May 2013