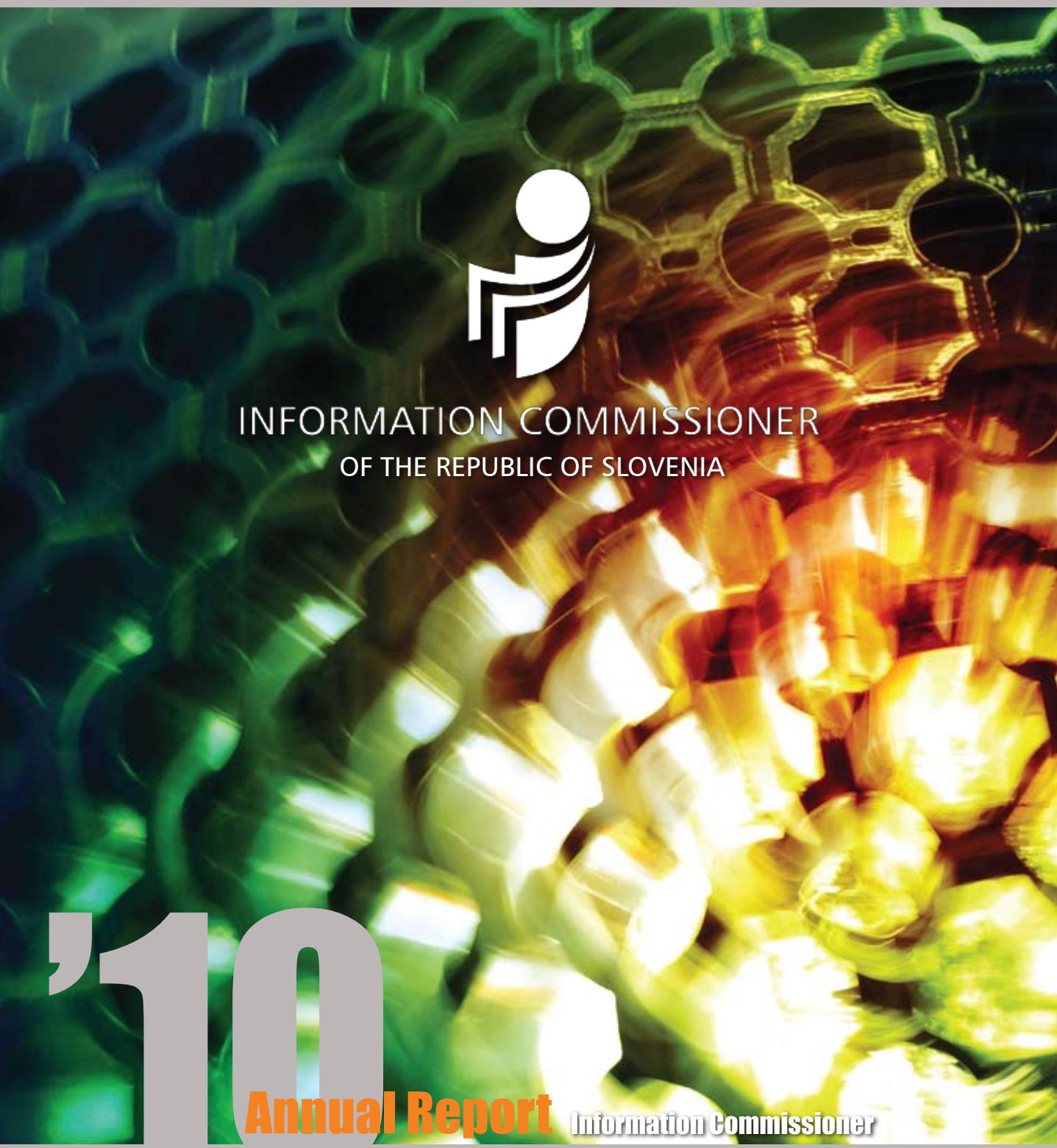


INFORMATION COMMISSIONER

OF THE REPUBLIC OF SLOVENIA

'10 Annual Report

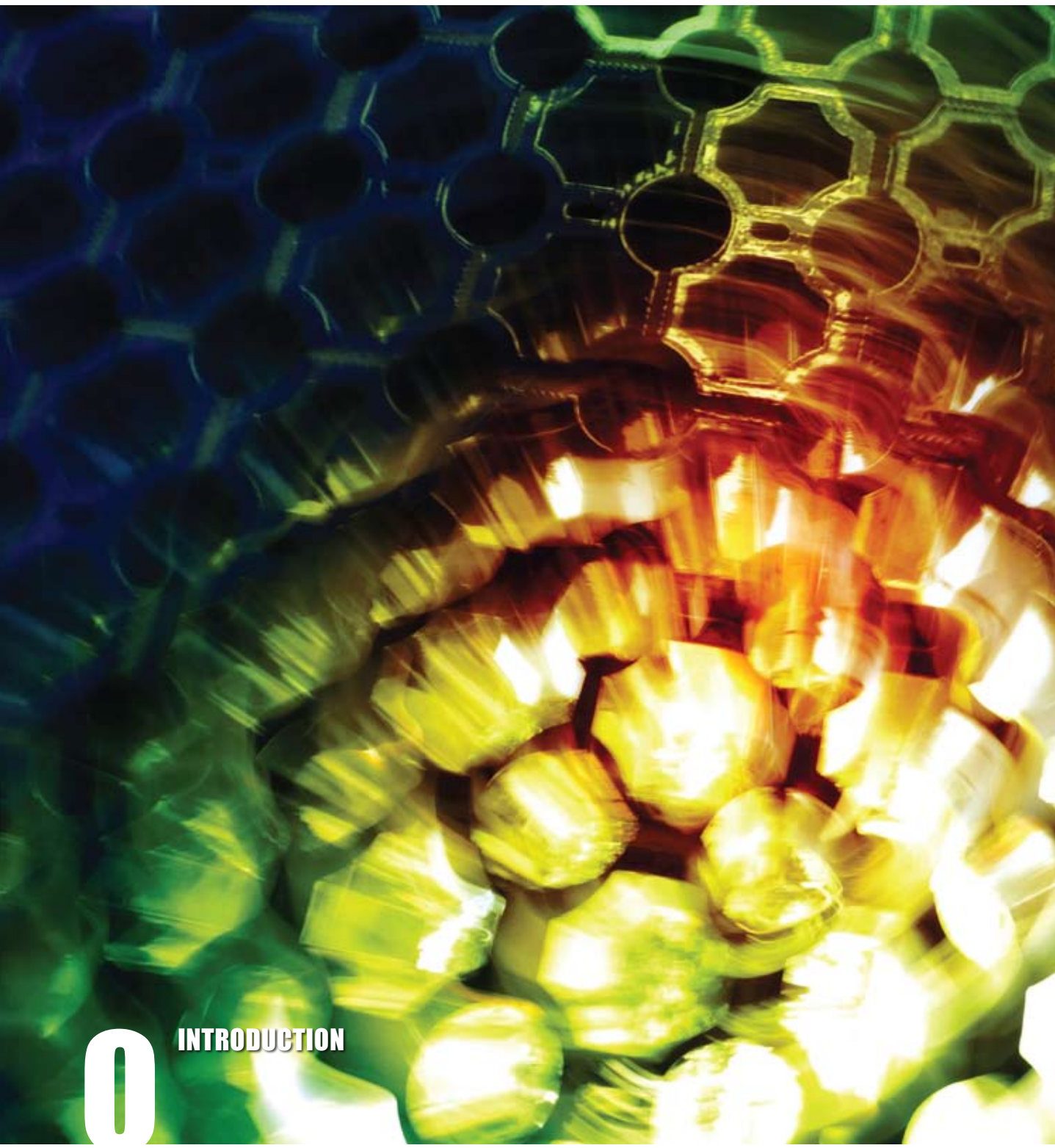
Information Commissioner

2010

'10 Annual Report

Information Commissioner

2010



0 INTRODUCTION

The year 2010 was marked by a noticeable increase in individuals' level of awareness of the importance of the right to access public information and the right to personal data protection. I can conclude with satisfaction that Slovenia is becoming a society of well informed and aware individuals who increasingly understand the purpose and importance of these two human rights whose implementation and protection fall within the competence of the Information Commissioner. Greater sensitivity to the issues regarding access to public information and personal data protection is reflected in the ever greater scope of cases received by the Information Commissioner, regarding either requests for an opinion, complaints, or appeals. In our work we strive to be as responsive and professional as possible, which the public recognises 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 February 2010 the level of trust in the Information Commissioner was characteristically high (53.1%), while the level of distrust was the lowest of all the institutions monitored (12.2%). Of such institutions, only the Euro was marked by a slightly higher level of trust (54%). Since previous measurements also demonstrated a high level of trust (November 2009 – 44%; March 2009 – 46%) 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, observations have been similar from year to year. It may still occur that an applicant does not receive an answer due to the fact that a authority not only does not provide a document that the applicant has requested, but also does not take the time to respond. It may also still happen that an authority "does not feel obliged" to decide in accordance with the Access to Public Information Act (hereinafter: APIA). With regard to the implementation of the APIA, also in 2010 the Information Commissioner often noticed the problem of high fees being charged for providing public information – fees covering the costs of the work of the civil servants who find and prepare the information for the applicant. The Information Commissioner already warned of such conduct in the last two annual reports. Unfortunately, the authorities did not take such warnings seriously enough. In my opinion, the fees for access to information should be as low as possible. The APIA namely ensures everyone free access to public information documents; when photocopies of such need to be provided, the liable authority may only charge for material costs. It seems that sometimes by charging high fees authorities attempt to reduce the number of requests or the scope of such. I must emphasise that this concerns the exercise of a fundamental human right; authorities are obliged to enable such right and make its exercise easier and not more difficult by applying various measures that burden applicants.

In the area of personal data protection, in 2010 the Information Commissioner called attention to the further increase in the use of technological means to process personal data. Often uncritically, with insufficient consideration, and above all without a legal basis, data controllers are increasingly often deciding to record phone calls and to carry out video surveillance. Information technology today enables ever more subtle interferences with the privacy of individuals. It is possible to rapidly process an enormous amount of data, to classify it according to various criteria, segment it, combine it, etc. The ease and speed of procedures for processing personal data and the affordability of technology inevitably leads to a greater appetite for such, encourages the desire for broader (more detailed) insight into the individual and his legal status and personal circumstances – including in areas where this is not expected, i.e. in schools, associations, and smaller businesses, such as beauty and hair salons.

Therefore it is all the more likely that the quote: "Privacy is dead! Get over it!" applies. Many people wave off the legal restrictions and discussions such as this one with the argument: "If you have nothing to hide, you have nothing to fear." They should be afraid of this very argument as it stems from the presumption that the individual is trying to hide something bad or forbidden. But that is not what privacy is about. Before the fall of the Iron Curtain, privacy was understood as being connected with democratic society. The more democratic society was, the less it intruded upon the private sphere of the individual. However, in the democratic society of today, not only the state, i.e. the authority, intrudes upon privacy (above all information privacy) by frequently disproportionate collection and processing of personal data, but it is increasingly also the private sector, commercial companies, banks, insurance companies, etc., who do so.

Since one cannot turn back the clock – and why would one even try to do so when new technological solutions are primarily beneficial for business – it is necessary to ensure that technology be designed in such a manner that it will have the least impact on the privacy of individuals. And that tools be used that will enable privacy to be built into technologies (by means of the so-called Privacy by Design method).

In 2010 the Information Commissioner devoted a great deal of attention to preventative activities. For the individual fields that are the most problematic in practice it issued a number of new guidelines in Slovene which will be of help to users (Privacy Impact Assessments; Guidelines for Personal Data Protection in Online Forums; Guidelines for Health Care Service Providers; Guidelines for the Development of Information Solutions), and throughout the year it provided for the public nature of its work and raised the awareness of legal entities and natural persons by means of regular contact with the media, through its website, and naturally by means of direct communication with liable entities. Experts at the Information Commissioner participated in a number of educational conferences, congresses, and round tables. Once again last year the Information Commissioner marked Personal Data Protection Day and International Right to Know Day with a variety of activities.

On the legislative level, in 2010 I was somewhat disappointed with how quickly the ministries (and legislature) decided to link the filing systems in the eSociala (e-Social Services) project. I am still of the opinion that a more effective, privacy-friendly, and also cheaper solution should have been sought by simplifying the system for recognising the right to and allocating social transfers. I am convinced that it is not possible to "simplify" a complex solution in terms of content by linking the currently largest number of personal data filing systems in the public (as well as private) sector. The project led to the establishment of personal data filing systems at data controllers who in fact do not need such, just so that the data will be available for linking and carrying out tasks in connection with social transfers. For instance, one of the filing systems should also process data on the average grades of children, although it is known that such are needed only in the procedure for deciding on entitlements and the amount of scholarships which only a relatively low percentage of youths in schooling are granted. The trend of establishing new personal data filing systems and "enriching" already existing ones with new personal data is very present in the public sector and is raising concern. It seems that no one ever believes anyone anymore, it is always necessary to supervise and check everyone. It worries me that we do not all share a fear of the surveillance society, which Slovenia could quickly transform into if the above-described orientation and conduct continue. When the individual no longer has space for privacy because his personal data areis processed without his knowledge and to a dispro-

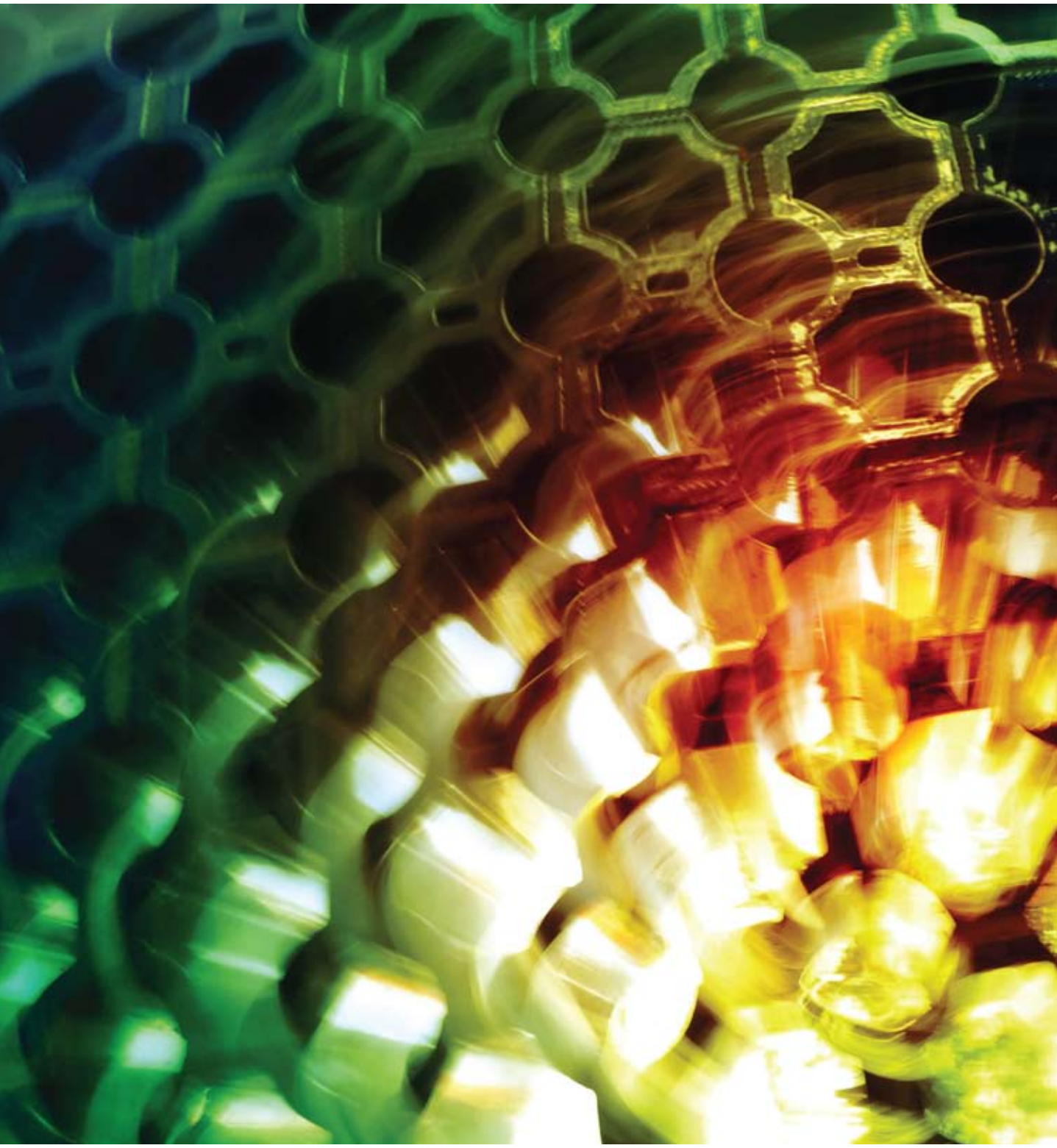
portionate extent, and employers, banks, shops, and the state raise intimate questions and make video and audio recordings of him, it is the end of freedom. I hope that the readers of this report will also consider these issues.

I also hope that those who have the possibility to decide realise that depriving the Information Commissioner of the possibility to access the Constitutional Court, especially in the information society, will not bring about anything good.

Yours sincerely,

Nataša Pirc Musar
Head of the Information Commissioner

KAZALO/CONTENTS



1 THE INFORMATION COMMISSIONER

1.1. Establishment of the Information Commissioner

On 30 November 2005 the National Assembly of the Republic of Slovenia adopted the Information Commissioner Act[1] (hereinafter: the ICA), on the basis of which an autonomous and independent state authority was established on 31 December 2005. The aforementioned Act merged two authorities, the Commissioner for Access to Public Information, which prior to that had the status of an independent authority, and the Inspectorate for Personal Data Protection, which had operated as a constituent authority within the Ministry of Justice. Upon the implementation of the ICA, the Commissioner for Access to Public Information continued its work as the Information Commissioner, whereby the inspectors and other employees of the Inspectorate for Personal Data Protection and its equipment and resources came under its competence. Concurrently, it also assumed responsibility for all pending cases, archives, and records of the Inspectorate for Personal Data Protection. Thus, the jurisdiction of the authority that had previously been responsible for ensuring unimpeded access to public information transformed and expanded to encompass personal data protection. In such a manner, the Information Commissioner became a national supervisory authority for personal data protection and commenced operations on 1 January 2006.

With such regulation, which is comparable to that of other developed European states, the practices of the two authorities became uniform, and today awareness of the right to privacy and the right to know continues to increase, rights which as a result of this regulation are ever more harmonised.

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. The Head of the Information Commissioner is Nataša Pirc Musar.

1.2. Competences of the Information Commissioner

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 thereunder (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

[1] Zakon o Informacijskem pooblaščencu, Official Gazette RS, No. 113/2005 – 51/2007–ZUstS-A.

competences determined by Article 45 of the Public Media Act[2] (hereinafter: the PMA). In accordance with 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 lack of a response of an authority following such a request is a violation and grounds for an appeal. The Information Commissioner decides on an appeal against a decision refusing a request in accordance with the provisions of the Access to Public Information Act[3] (hereinafter: APIA).

The Information Commissioner is also the authority competent to determine and punish offences and to carry out supervision with regard to the implementation of the Information Commissioner Act, the Access to Public Information Act with regard to the appeals procedure, Article 45 of the Public Media Act, and the Personal Data Protection Act[4] (hereinafter: PDPA-1).

The Information Commissioner also has the following competences on the basis of the Electronic Communications Act[5] (hereinafter: the ECA):

to carry out inspections of retained traffic and location data acquired or processed in connection with providing public communication networks or services in accordance with Articles 107.a to 107.e of the ECA (the second paragraph of Article 112 of the ECA);
in the area it supervises, to decide on offences due to a violation of the ECA and regulations issued on the basis thereof, as the authority competent to determine and punish offences in accordance with the act regulating offences (Article 147 of the ECA);
to prevent abuses of and proper implementation of the European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and the amended directive on the retention of telecommunications data, which was adopted in Brussels on 15 December 2005 on the proposal of the ministers of the Member States.

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 so-called Schengen Convention (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. On the basis of Article 114 of the Schengen Convention, each Contracting Party shall designate a supervisory authority responsible in accordance with national law for carrying out independent supervision of the data file of the national section of the Schengen Information System (hereinafter: SIS) and for checking that the processing and use of data entered in the SIS does not violate the rights of the data subject. A joint supervisory authority is competent to supervise the implementation of the technical support function of the SIS with regard to personal data protection, while national supervisory authorities are responsible for supervising the national data files of the Contracting Parties, being in Slovenia the Information Commissioner.

In 2008 the Information Commissioner acquired competences pursuant to the Patients Rights Act[6], the Identity Card Act[7], and the Travel Documents Act[8].

On the basis of the Patients Rights Act (hereinafter: the PRA), the Information Commissioner has the following competences:

- to decide on appeals by patients and other entitled persons in cases of a violation of the provision regulating the manner of access to medical records; in this procedure the provider of health care services is regarded as the first instance authority (the tenth

[2] Zakon o medijih, Official Gazette RS, No. 110/2006, official consolidated text 1 with amendments.
[3] Zakon o dostopu do informacij javnega značaja, Official Gazette RS, Nos. 51/2006 and 117/2006-ZDavP-2.
[4] Zakon o varstvu osebnih podatkov, Official Gazette RS, No. 94/2007 - official consolidated text.
[5] Zakon o elektronskih komunikacijah, Official Gazette RS, No. 13/2007 official consolidated text 1 with amendments.
[6] Zakon o pacientovih pravicah, Official Gazette RS, No. 15/2008.
[7] Zakon o osebni izkaznici, Official Gazette RS, No. 71/2008 – official consolidated text 2.
[8] Zakon o potnih listinah, Official Gazette RS, No. 62/2009 – official consolidated text 3.

paragraph of Article 41 of the PRA);
- to decide on appeals by persons defined by the Act against partial or total refusal of any request for access to medical records following the death of a patient (the fifth paragraph of Article 45 of the PRA);
- to decide on appeals by entitled persons against partial or total refusal of any request for access which refers to the duty to protect information on the medical condition of a patient, provided that it concerns information which originates from medical records (the seventh paragraph of Article 45 of the PRA).

On the basis of the Identity Card Act (hereinafter: ICA), the Information Commissioner has the following competences:

- to carry out supervision of the implementation of Article 3.a of the ICA, which regulates the instances and manner in which the data controller is permitted to copy personal identity cards, and determines the manner in which copies may be stored;
- in the event of a violation of the provision of Article 3.a of the ICA, to determine and punish the offence as the competent authority, in accordance with Article 19.a of the ICA.

On the basis of the Travel Documents Act (hereinafter: TDA), the Information Commissioner has the following competences:

- to carry out supervision of the implementation of Article 4.a of the TDA, which regulates the instances and manner in which the data controller is permitted to copy passports, and determines the manner in which copies may be stored;
- in the event of a violation of the mentioned Article 4.a of the TDA, to determine and punish the offence as the competent authority, in accordance with Article 34.a of the TDA.

In 2009, the Information Commissioner also gained the following competences under the Banking Act[9] (hereinafter: BA):

- to give its consent to the administrators of the SISBON system prior to the application of the system's rules referred to in point 1 of paragraph 13 of Article 309.a of the BA, which determines that the administrator must adopt the rules of the system, wherein he determines the technical conditions for members, i.e. banks, to access the system and other measures for the security of personal data (paragraph 14 of Article 390.a of the BA);
- to carry out supervision of the implementation of Article 309.a of the BA, which regulates the collection, processing, and system of exchange of information on the credit rating of clients (the SISBON system) and, in accordance with Article 397 of the BA, to conduct procedures deciding on offences due to violations of Article 309.a of the BA (paragraphs 10–15 of Article 397 of the BA).

1.3. Organisation of the Information Commissioner

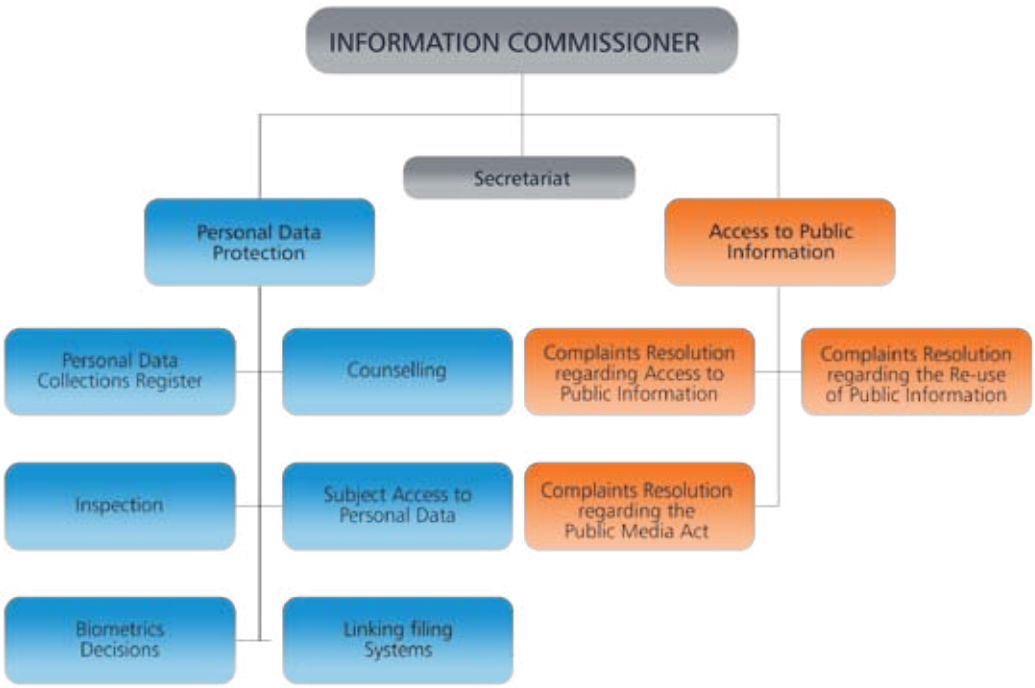
The internal organisation of the Information Commissioner and the structure of professional positions therein required to carry out its tasks are determined by the Act on the Internal Organisation and Post Classification of the Information Commissioner and the annex thereto, i.e. the Classification of Posts within the Information Commissioner. The classification of positions is adapted to the tasks and duties of the Information Commissioner and the work processes carried out therein, and is designed such that it ensures the most effective use of human resources.

[9] Zakon o bančništvu, Official Gazette RS, No. 131/2006, with amendments.

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

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

Figure 1: Organisational Chart of the Information Commissioner.



At the end of 2010, the Information Commissioner had 34 employees, of which five were employed on the basis of temporary contracts. Three of the temporary employees were substituting for employees on leave, while two were trainees. The number of workers employed at the Information Commissioner increased slightly in comparison to 2009. All employees in official positions have at least a bachelor's degree.

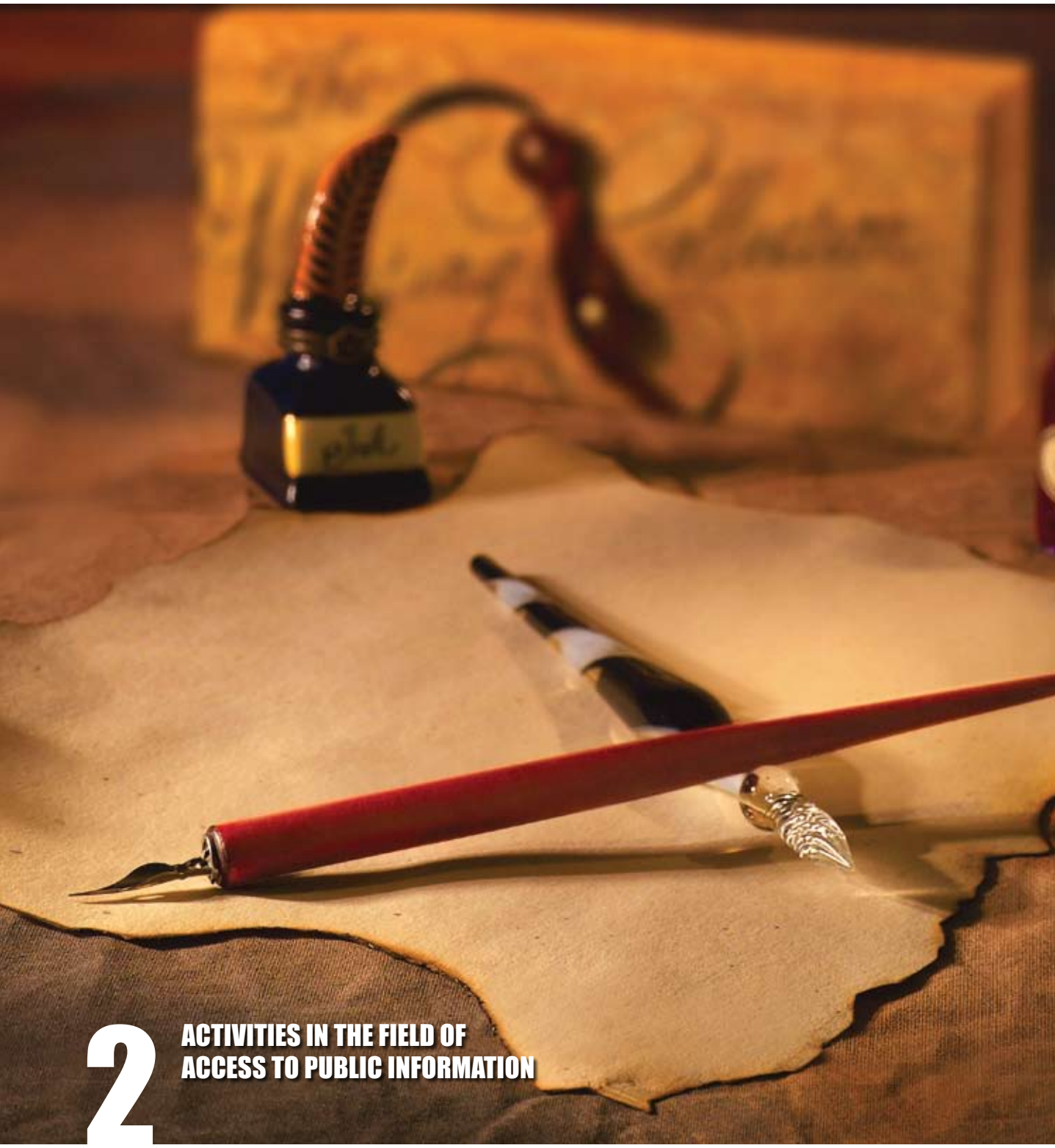
1.4. Budget of the Information Commissioner

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 Information Commissioner Act). In fiscal year 2010, the funding allocated to the Information Commissioner at the start of the year amounted to EUR 1,421,664.68. Of this, EUR 895.45 was brought forward from the previous year's allocation, under Budgetary Items 7459 and 7460, as well as EUR 5,974.53 of European funding from the European Privacy Open Space project, under Item 9378. During the year the Information Commissioner received EUR 11,400.00 of European funding for participation in the LAPSI project, under Item 9586. Of these funds, EUR 6,628.34 were used in 2010, while the remaining funds were brought forward to 2011. At the end of 2010, the Information Commissioner received EUR 67,407.60 of European funding for participation in the Twinning project, of which EUR 2,524.80 was used in 2010, with the remainder brought forward to 2011. In order to increase savings in the state budget, the Information Commissioner returned EUR 13,000.00 to the budget from Item 1267 (wages and salaries). The Information Commissioner reassigned EUR 2,113.51 from Item 1271 (material costs and expenses) to Item 1273 (investments), and 1,500.00 EUR to Item 1267 (wages and salaries).

In 2010, the Information Commissioner used EUR 1,386,158.63 of budgetary funding, of which:

- EUR 1,038,430.43 for wages and salaries and other employee expenses;
- EUR 325,614.69 for material costs and expenses;
- EUR 22,113.51 for investments and capital expenditure.

The operational budget at year end amounted to EUR 1,502,972.58. European funds for the implementation of the LAPSI and Twinning projects are included in this amount. Excluding earmarked and European funds, 98.88% of the budget was used, while the figure is 94.27% taking into account incomings due to European funding.



2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

2.1. Legislation on Access to Public Information in the Republic of Slovenia

The legislature ensured the right to access public information in the Constitution of the Republic of Slovenia[10]. The second paragraph of Article 39 of the Constitution determines that "Except in such cases as are provided by law, everyone has the right to obtain information of a public nature in which they have a well founded legal interest under law." Even though the right to access public information is a fundamental human right, and was, as such, included in the Constitution, it was not until eleven years after the Constitution had been adopted that this right was implemented through the adoption of the 2003 Access to Public Information Act[11] (hereinafter: APIA). Until then, individual provisions with regard to public information had been part of certain disparate pieces of legislation; they became comprehensively regulated only by the adoption of the APIA. This Act was adopted by the National Assembly of the Republic of Slovenia in February 2003, and entered into force on 22 March 2003.

A step forward was made in 2005 through the adoption of an amendment to the APIA. The amendment namely decreased the possibility of unjustified denial of access to information and introduced numerous novelties, such as the re-use of public information and the competences of the administrative inspectorate in the implementation of this Act. The public interest test was the most important novelty. The amendment also emphasised the accessibility of data on the use of public funds as well as data concerning employment and the performance of public office. Thereby Slovenia joined those democratic countries in which, as regards the public interest, exceptions are treated with reservation.

2.2. Review of Activities in the Field of Access to Public Information in 2010

In 2010 the Information Commissioner received 592 appeals, of which 231 were against decisions refusing requests, while 361 were against the non-responsiveness of first-instance authorities.

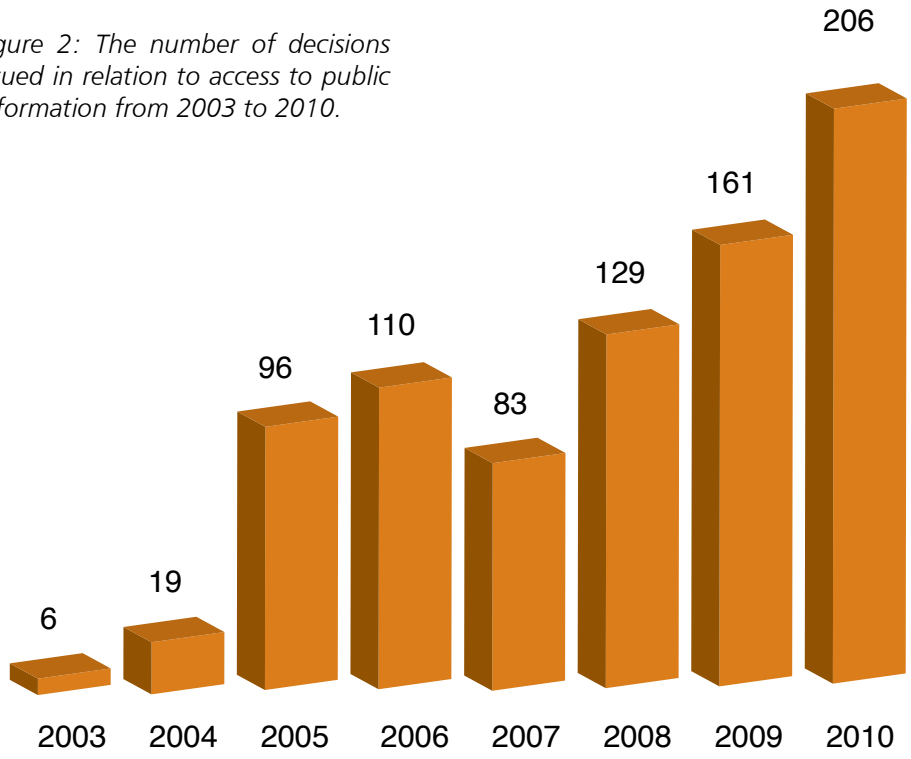
In appeal procedures against decisions by which authorities refused requests for access to or the re-use of public information, the Information Commissioner issued 206 decisions (31 of which related to cases the Information Commissioner received for consideration in previous years); in 6 cases it issued a decision rejecting the appeal; 7 cases were transferred to a competent authority for consideration; and 5 applicants withdrew their appeal. In appeal procedures against non-responsiveness, the Information Commissioner first called on to the liable authorities, to decide on the requests as soon as possible. In 275 cases the liable authorities did make a decision regarding the applicant's request upon being called on to do so by the Information Commissioner and in the majority of cases they provided the applicant with the requested public information. Procedures addressing non-responsiveness were concluded by means of a response from the liable authority, while the applicants who thereby received decisions refusing their requests were able to appeal to the Information Commissioner on the basis of their request for access to public information being refused. In one case the liable authority did not respond after being called on to do so by the Information Commissioner, following which the Information Commissioner took up the case for consideration and issued a decision. In 26 cases the Information Commissioner issued a decision rejecting the appeal on the grounds that the application had been submitted prematurely or was incomplete; to 3 applicants it issued the explanation that it was not competent to consider their applications; and 11 applicants withdrew their appeals.

[10] Ustava Republike Slovenije, Official Gazette RS, Nos. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, and 68/2006.

[11] Zakon o dostopu do informacij javnega značaja, Official Gazette RS, No. 24/2003.

In comparison with 2009, the number of decisions issued in relation to access to public information increased significantly. In 2009, 161 decisions were issued, whereas in 2010 the number of such was 206, of which 31 were related to cases that the Information Commissioner had received for consideration in previous years.

Figure 2: The number of decisions issued in relation to access to public information from 2003 to 2010.



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

- in 69 cases it granted the appeal of the applicant;
- in 63 cases it dismissed the appeal;
- in 49 cases it partially granted access to information;
- in 21 cases it returned the matter to the first instance authority for reconsideration;
- in 4 cases it rejected the appeal.

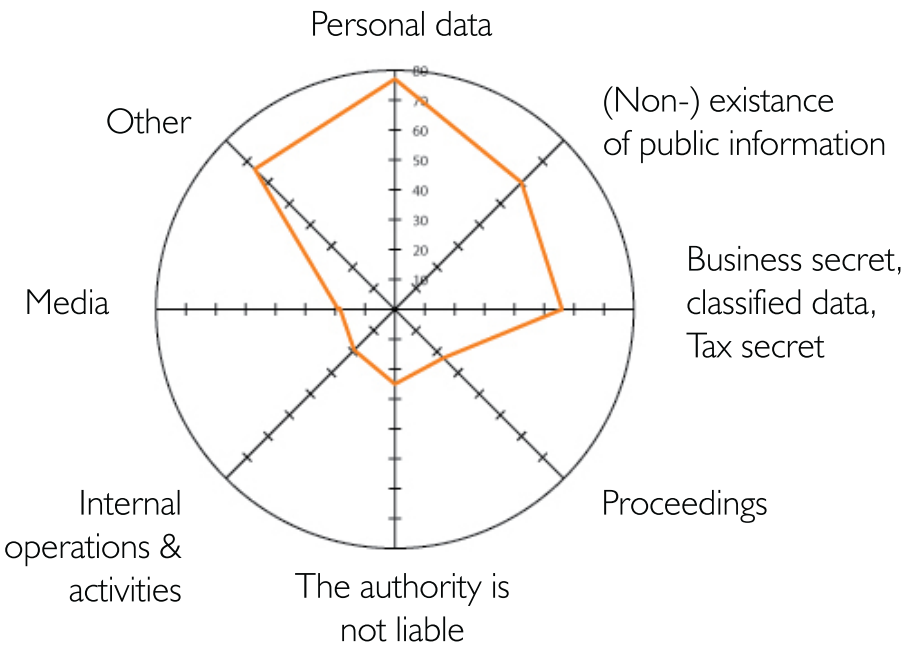
In its decisions the Information Commissioner considered and decided upon the merits of the following:

- whether the documents requested contained personal data whose disclosure would entail a violation of the PDPA-1 (77 cases);
- whether the liable authority even possesses the document or the public information requested by the applicant (60 cases);
- whether the applicant requested information and/or data deemed to be a business secret in accordance with the Companies Act (41 cases);
- whether the authority to whom the request for access to public information was addressed is at all liable under the first paragraph of Article 1 of the APIA (24 cases);
- whether a violation of procedural rules occurred (23 cases);
- whether the information requested pertains to data in documents compiled in relation to the internal operations or activities of the authority and whose disclosure would interfere with the functioning and activities of the authority (19 cases);

- whether a decision was issued in procedures where the applicant was a journalist or media entity (18 cases);
- whether the document requested meets the conditions for it to be deemed public information under the first paragraph of Article 4 of the APIA (12 cases);
- whether a decision was issued in procedures in which the applicant requested documents related to public procurement procedures (11 cases);
- whether the information requested pertains to data obtained or compiled on the basis of a criminal prosecution or in relation to such or on the basis of an offence procedure, and whose disclosure would be detrimental to the course of prosecution or the procedure (11 cases);
- whether the public interest in disclosure is stronger than the public interest or the interest of other persons in restricting access to the information requested (8 cases);
- whether the information requested pertains to data in documents that are still in preparation and are thus subject to internal discussion, and the disclosure of such documents would lead to misinterpretation as to their content (7 cases);
- whether authorities charged correct fees for providing public information (7 cases);
- whether entities violated substantive law (7 cases);
- whether the information requested pertains to data classified as confidential in accordance with the Classified Information Act (6 cases);
- whether an entity must reduce the level of confidentiality of the document requested (6 cases);
- whether the information requested is protected in accordance with the act regulating copyright – in such instances the applicant is enabled access to the information by allowing him to view it (5 cases);
- whether the information requested pertains to data that was obtained or compiled on the basis of civil or non-contentious civil proceedings, or any other judicial proceedings, and the disclosure of such would be detrimental to the course of such proceedings (4 cases);
- whether the information requested pertains to data whose disclosure would entail a violation of the confidentiality of a tax procedure or tax secrecy, in accordance with the act regulating tax procedure (2 cases);
- whether the information requested pertains to data that was obtained or compiled due to an administrative procedure and whose disclosure would be harmful to the course of the procedure (1 case);
- whether the re-use of certain public information is at issue (1 case);
- whether a right determined by the APIA is at issue (1 case);
- whether the case concerns the proactive publication of information (1 case).

In 2010, the Information Commissioner issued seven decisions in cases from previous years in which an appeal had been lodged with the Administrative Court, which ruled that the Information Commissioner must decide again with regard to the cases in question.

Figure 3: Decisions related to the APIA with regard to various exemptions. (Note: One decision may refer to several exemptions.)



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

- ministries, constituent bodies, and other state authorities (79 cases);
- public funds, institutes, agencies, and other entities under public law (47 cases);
- public administration units, municipalities, and local communities (37 cases);
- courts, the State Prosecutor's Office, the State Attorney's Office (27 cases);
- health care institutions (10 cases);
- educational institutions (3 cases).

Three appeals referred to legal entities in the private sector, however it was established that they are not liable authorities under the APIA.

125 applications were submitted by natural persons, 60 by private sector legal entities, of which 21 were either non-governmental organisations, societies, or associations. 18 complaints were submitted by journalists and 3 by public sector legal entities.

In considering appeals, sometimes it is necessary to arrange an examination in the absence of the party requesting access to public information, a so-called in camera examination, by means of which the Information Commissioner can establish the actual state regarding documents held by the authority. In 2010, 82 such examinations were carried out.

In 2010, 31 appeals were filed with the Administrative Court against decisions of the Information Commissioner (i.e. against 15% of the decisions issued). The relatively small portion of such appeals, which has remained at the same level for a number of 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 2010 the Administrative Court issued 31 judgments in relation to appeals filed against the decisions of the Information Commissioner. In 16 cases

it dismissed the appeal, in 13 cases it granted the appeal, annulled the contested decisions and returned the matter to the Information Commissioner for reconsideration, and in 2 cases it decided partially in favour of the appellants such that it partially annulled the contested decision and returned it for reconsideration to the Information Commissioner; it dismissed the remainder. In 2010 three requests for a revision were filed with the Supreme Court against the decisions of the Administrative Court. In 2010 the Supreme Court decided one such case and rejected the request for a revision.

In 2010, the Information Commissioner received 382 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.

In 2010 one procedure was initiated with regard to offences due to a violation of the first paragraph of Article 10 of the Information Commissioner Act (hereinafter referred to as: the ICA), since the liable entity did not provide the requested documents to the Information Commissioner. The Information Commissioner did not find any violations of Article 23 of the APIA or Article 45 of the Media Act.

2.3. The Most Significant and Precedent Cases in Different Areas

Procedural fees

By Decision No. 021-111/2008/9, dated 22 January 2010, the Information Commissioner decided following a judgment issued by the Administrative Court ordering the Information Commissioner to decide on the merits of an appeal against a decision regarding the fee charged by a first instance authority for providing public information. The Information Commissioner followed the instructions of the Court and considered the merits of the contested decision, namely whether the authority had grounds for charging the fee. It is clearly specified in the law that authorities must publish their schedule of fees referred to in Article 35 of the APIA in their public information catalogues, which had not been done in the case at issue. The Information Commissioner decided that the authority did not have any basis for applying the schedule of fees of the Ministry of the Economy when charging the fee, irrespective of the fact that the authority at issue is a constituent part thereof. The Information Commissioner granted the appeal of the applicant and itself determined the fee for providing the public information.

Reducing the level of confidentiality

By Decision No. 090-181/2009/3, dated 25 January 2010, the Information Commissioner for the first time adopted a decision on the basis of the third paragraph of Article 21 of the APIA, regarding the question of whether it is justified for certain documents to be classified as confidential in accordance with the Classified Information Act. The applicant requested that the authority reduce the level of confidentiality of a document classified as CONFIDENTIAL. The authority adopted a decision refusing the request on the grounds that it follows from the assessment of the confidentiality level that the procedure for accepting the credentials of an ambassador is not of a public nature. The authority claimed that the public consideration and analysis of the possible existence of a justified basis for accepting credentials in specific procedures for appointing foreign ambassadors to the Republic of Slovenia would bring about harmful consequences for bilateral relations between the Republic of Slovenia and the appointing state, and thus also for the economic, political, and other interests of the Republic of Slovenia. The Information Commissioner decided that the two documents at issue fulfilled the formal condition to be classified as confidential

but not the substantive condition since they do not at all concern any of the informal procedures for appointing foreign ambassadors to the Republic of Slovenia (neither specific nor general), to which the Minister of Foreign Affairs and the Secretary-General of the Government referred in their assessments. The Information Commissioner granted the appeal and annulled the contested decision due to the incorrect application of substantive law.

Internal functioning of an authority

By Decision No. 090-3/2010, dated 29 January 2010, the Information Commissioner decided on an appeal against the decision of the Office of the President of the Republic of Slovenia which partially refused an applicant's request to be provided access to all the letters sent over the past year by the President of the Republic to the Prime Minister of the Republic of Slovenia, and the letters received by the President of the Republic from the Prime Minister. Upon examining the letters requested, the Information Commissioner determined that they had not been produced in procedures that fall within the formal competences of the President of the Republic as determined by the Constitution and the valid legislation, and that they served the purpose of internal communication between the President of the Republic and the Prime Minister. The Information Commissioner deemed the letters to be documents produced in relation to the internal functioning and operations of the President of the Republic and the Prime Minister. At the same time, it established that the content thereof does not comprise facts regarding the functioning of the two institutions, but rather the letters contain informal standpoints, proposals, initiatives, and opinions expressed by the President of the Republic to the Prime Minister on topics the President deemed to be important in a broader social sense. Thus, the situation concerned open communication between the two most important public office holders in the state, which by its nature requires a certain degree of confidentiality. The Information Commissioner determined that both conditions were fulfilled for the existence of an exception from free access to public information under point 11 of the first paragraph of Article 6 of the APIA and it dismissed the applicant's request in its entirety.

The re-use of public information

The applicant requested that the authority provide information from the land cadastre and the Consolidated Cadastre of Public Infrastructure. The stated purpose regarding the use of the information was "geodetic services" and "carrying out public tasks in accordance with public authorisation"; namely, to formulate the national spatial plan, entitled "DLN 110kv Grosuplje-Trebnje". The authority issued a decision charging the applicant a fee for the re-use of geodetic information for a commercial purpose. In its appeal, the applicant claimed that it should be entitled to an exemption from paying the fee since the information was intended for use by state authorities. The Information Commissioner found that on the basis of the request and appeal of the applicant it was not possible to establish which public task would be carried out by using the information requested and it therefore concluded that the condition determined by the third paragraph of Article 4 of the APIA, which defines the term "the re-use of public information", had not been fulfilled. On the basis of these findings, the Information Commissioner dismissed the appeal by Decision No. 090-114/2009/2, dated 5 February 2010.

Personal data

By Decision No. 090-106/2010, dated 9 September 2010, the Information Commissioner granted the appeal of an applicant who requested that an authority provide a list of employees containing the following data: first name, family name, education, work position, salary bracket, and gross salary for the period January – March 2010, the list of contractors (first name, family name or title, the type of contract – author's contract or

subcontractor's contract, the subject of the contract, the overall amount paid to them in 2009, and the amounts paid to them in the period January – March 2010, if any), and the list of external contractors (first name, the subject of the contract, the total amount paid to them in 2009, and the amounts paid to them in the period January – March 2010, if any). The Information Commissioner found that such documents are held by the authority and that they suit the definition of freely accessible public information. In the case at issue, no exemption to personal data protection applies since it concerns data in relation to the employment of civil servants and data regarding the use of public funds.

Business secrets, the public interest test

By Decision No. 090-161/2009/15, dated 22 January 2010, the Information Commissioner granted an appeal against a decision of the Ministry of Health which refused the applicant's request to view a contract regarding the supply of pandemic influenza vaccine. The Information Commissioner found that, in accordance with the Companies Act, the document at issue was correctly labelled as a business secret. However, under European Union legislation, the components of a medicine which was granted marketing authorisation by the European Medicines Agency and included in the European Public Assessment Report (EPAR) can not be classified as a business secret. The Information Commissioner found that a certain part of the contract is a business secret and it therefore had to weigh whether public interest in the disclosure of that part of the contract is greater than the interest due to which such information is protected as a business secret. In Slovenia as well as throughout Europe the supply of the vaccine against the pandemic influenza H1N1 triggered numerous dilemmas and questions subject to debate within official institutions, the media, and also the broader public. Individuals who are considering vaccination or who have been vaccinated have the right to exhaustive and complete information on whether a vaccine is safe and what obligations and responsibilities the state has assumed under the contract on vaccine supply; if the situation entails the potential assumption of financial obligations by a state, it can consequently involve all taxpayers. The question of what kind of obligations a state has assumed in such an important area as public health is always a matter of public interest, also for reason that such a responsibility can entail new financial consequences for the budget of the Republic of Slovenia, i.e. the use of public funds.

Whether an entity is liable under the APIA; business secrets; personal data

By Decision No. 090-206/2010, dated 22 November 2010, the Information Commissioner decided on the appeal of an applicant who requested that the Student Organisation of Slovenia (hereinafter: SOS) provide it with photocopies of the financial reports of the SOS and individual branches of the University from 1994 onward. The Information Commissioner first determined that the SOS is undoubtedly a legal entity under public law and is obliged to provide public information under the provisions of the APIA. The SOS is a bearer of public authority, its objectives and activities being of a distinctly public law nature; the SOS obtains funding from the state budget and the budgets of local self-governing communities through taxes and charges regulated by the state. The Information Commissioner also found that the SOS is not a business entity under the Companies Act and can therefore not apply the institute of the protection of business secrets to the documents produced in carrying out its tasks. The SOS is an entity under public law, founded in order to address issues of common importance and to realise the common interests of students, which entails that its operations must be transparent since its revenue and expenditure reflect indirect use of public funds. The Information Commissioner also decided that public financing is a fundamental reason why this authority's operations must be public to the greatest extent possible, including salaries, which are provided from public funds such as taxes. With regard to the SOS, the Information Commissioner assessed that personal data such as basic salaries, holiday bonuses, food and transportation reimbursement, etc., do not entail protected personal data and it therefore decided that the SOS must provide the applicant with the financial reports from 2003 onward.

2.4. Overall Assessment and Recommendations Regarding Access to Public Information

In 2010, the Information Commissioner saw an increase in cases related to access to public information. It received 974 cases (as compared to 812 in 2009) – as in the prior two years, the number of appeals in this area increased significantly. In 2010 the Information Commissioner received 592 appeals, of which 361 were against the non-responsiveness of first-instance authorities, while 231 were against decisions refusing requests. The number of questions, initiatives, and requests for explanations regarding the application of the Access to Public Information Act (APIA) also increased (all together 382 cases, as compared to 328 cases in 2009). With regard to access to public information, the Information Commissioner functions as an appellate authority and is therefore not allowed to voice opinions in advance about specific issues that could become subject to the appellate procedures it decides on. Irrespective of the above-mentioned, the Information Commissioner provides liable authorities and applicants non-binding explanations regarding the procedure determined by the APIA and explanations in relation to cases the Commissioner has encountered in practice when deciding upon appeals.

On the basis of the appellate procedures carried out, the Information Commissioner assesses that liable authorities as well as applicants are more aware of possible ways to access public information, while liable authorities are publishing more information on the internet on their own, i.e. without applicants having to request such information. In 2010 the number of appellate procedures related to the exemption of confidential information increased; furthermore, for the first time since being established, the Information Commissioner conducted six appellate procedures in relation to requests for reducing the level of confidentiality. In the past such appeals had not occurred at all.

A common problem occurring in practice that the Information Commissioner noted also in 2010 in relation to the implementation of the APIA is the issue of the fees charged for providing information, which the Commissioner had already called attention to in the previous two annual reports. In 2010 the Information Commissioner found the following to be the most common irregularities in relation to fees charged for access to information:

- Liable authorities do not warn applicants beforehand that they will charge a fee for providing access to information, as provided for in the third paragraph of Article 36 of the APIA.
- Liable authorities do not have a schedule of fees approved by the ministry competent for administrative affairs, or the schedule of fees is not published in their catalogue of public information, however they still charge applicants a fee in accordance with the schedule of fees.
- Even upon the request of an applicant to be notified in advance on the envisaged fee, as provided for under the third paragraph of Article 36 of the APIA, liable authorities fail to fulfil this obligation, but they still charge the applicant a fee.

In relation to fees charged for accessing public information, the Information Commissioner explains that it follows from the APIA that liable authorities may charge a fee but they are not obliged to do so. The Information Commissioner is of the opinion that such a fee should be as low as possible (the APIA ensures free access to public information, however a fee covering material costs can be charged for providing photocopies) and it should not limit the exercise of this fundamental human right. In addition to the above-mentioned, it should also be emphasised that the right to access public information is provided for by the second paragraph of Article 39 of the Constitution. The purpose of the APIA, which follows from the basic principle of transparency, is reflected in the three functions of access to information, i.e. the democratic, economic, and supervisory functions. The Information Commissioner emphasises that the open nature of the operations of authorities cannot be limited only to various forms of parliamentary decision-making, but must also entail

various forms of direct participation of citizens in adopting regulations and political decisions. The institute of access to public information enables citizens to become familiar with the operations of authorities and to actively participate in the implementation of power. The supervisory function enables citizens to supervise the correctness of the work of the public administration and the work of authorities, thus enabling the prevention of poor management, the abuse of power, and corruption. Communication and a close relationship between the public administration and individuals strengthens the trust of the latter in the administration and also prevents individuals from perceiving adopted decisions as enforced, but rather they will understand them better and therefore accept them.

The Information Commissioner, as a constituent element of the public sector, acts in the spirit of openness and transparency also in implementing the competences of an appellate authority. Therefore, it attempts to introduce the principle of transparency in the appellate procedures it is competent for in the fields of access to public information and the re-use of information in the public sector. In this spirit, the Information Commissioner regularly and proactively publishes on its website decisions adopted in appellate procedures in accordance with the APIA, judgments of the Administrative Court, remarks regarding drafts of various laws, explanations, and news on these areas.

With regard to access to public information, the field of so-called proactive transparency is becoming increasingly important. This entails that authorities liable under the APIA provide the public with certain information of their own accord, i.e. without applicants requesting such. They are obliged to do such by Article 10 of the APIA, which regulates the publication of public information on the internet and determines that every authority liable under the APIA is obliged to publish the following public information on the internet:

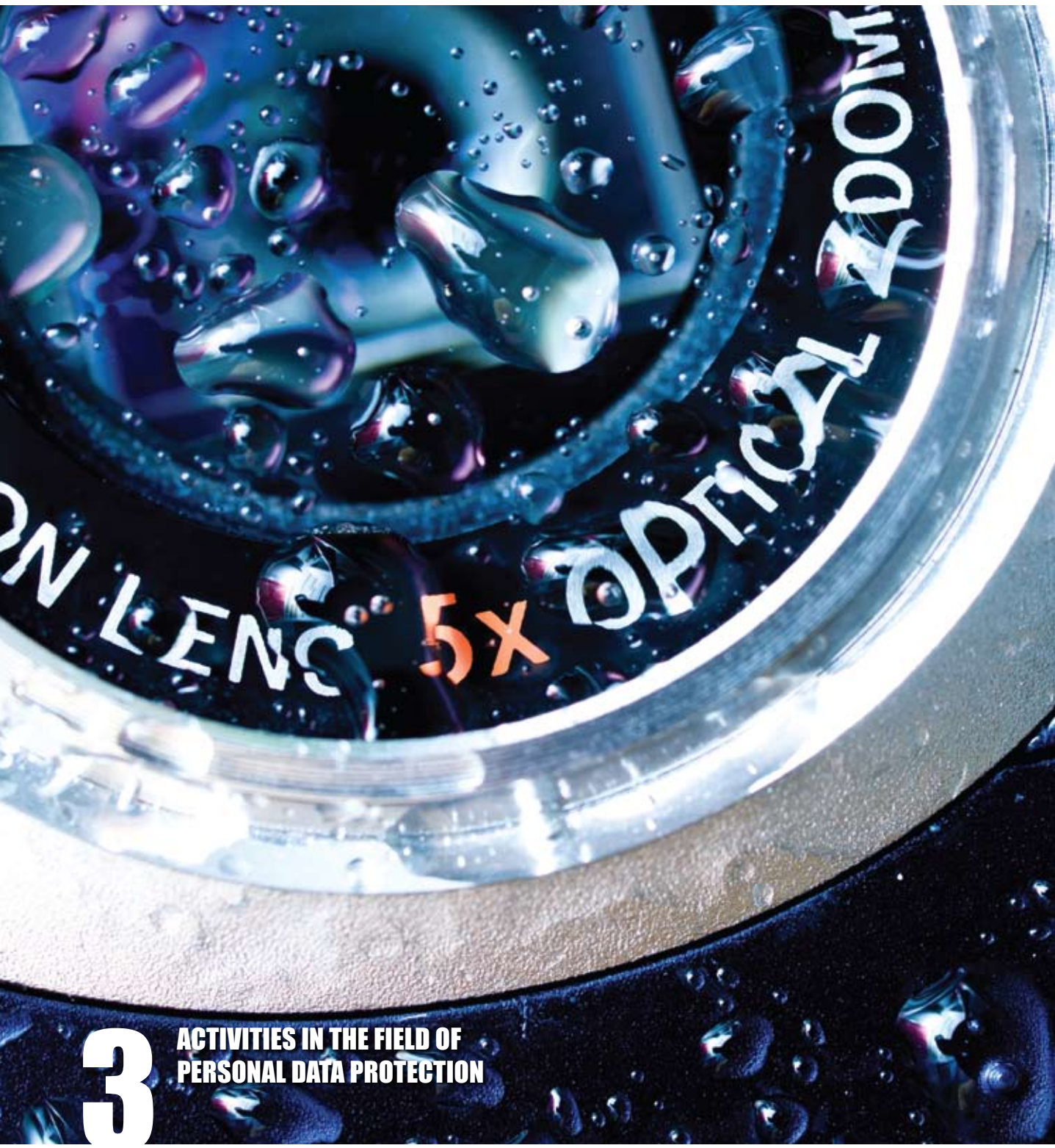
1. consolidated versions of regulations in relation to their field of work and linked to the national register of regulations published on the internet;
2. programmes, strategies, standpoints, opinions, and instructions of a general nature or of importance for the interactions of the authority with natural persons or legal entities, and for decision making regarding the rights or obligations of such; studies and other similar documents related to the field of work of the authority;
3. drafts of regulations, programmes, strategies, and other similar documents related to the field of work of the authority;
4. all published documents and documentation related to public tenders, in accordance with the regulations on public procurement;
5. information on the activities of the authority and on administrative, judicial, and other services it provides;
6. all public information that has been requested at least three times;
7. other public information.

Liable authorities must enable access to the above listed information free of charge.

In 2010 the Information Commissioner received only one appeal regarding the re-use of public information. In its opinion, there are several reasons for such, one of them being the fact that in practice this institute has not yet come fully to life, although interest in such – especially for the re-use thereof for commercial purposes – is increasing. Therefore, the Information Commissioner advises liable authorities to pay more attention to actively informing the public regarding the possibilities of the re-use of public information. Such entails the use of information by natural persons or legal entities for commercial or non-commercial purposes other than the initial purpose related to the public task for which the documents were created. The use of information by an authority or the exchange thereof between authorities in carrying out public tasks does not constitute re-use. The institute of re-use results in greater transparency and a more definite nature of information that commercial and non-commercial users obtain from the public sector. Public sector authorities collect, produce, reproduce, and distribute documents in order to perform public tasks they are responsible for as determined by the applicable regulations. The use of such documents for purposes other than the initial purpose constitutes re-use. The objective of

such is adding value to public information in that the private sector (applicants) should offer more or something other than authorities do in carrying out their public tasks. The purpose of further use and exploitation of public information is that applicants upgrade such and thus realise the economic function of the right to access public information. The economic function entails the importance of public information for the economy, as the re-use thereof helps create a market of public sector information as one of the key markets in spreading communication technologies. Understanding the importance of such a market occurring is essential for the development of re-use. Thus, primarily commercial users will process the information obtained, give it added value, and then offer such enriched information on the market again; however, they are not at all obliged to provide such enrichment by the law, but by the market. The public sector, or, more specifically, individual authorities, have the right, under the first paragraph of Article 34.a of the APIA, to charge a fee for the re-use of public information for commercial purposes; this, however, entails that such may charge a fee but are not obliged to do so. What is also important is the prohibition of discrimination with regard to applicants, which entails that the re-use of information for the same fee and under the same conditions is allowed and must be enabled to all applicants. Given the positive effects of re-use, it would make sense for liable authorities to start actively promoting such. In addition to this, the provision that liable authorities should publish in advance on the internet all the conditions regarding the re-use of information, namely the usual fees and the basis for calculating such in the event of special requests for re-use, should be respected without exception.

With regard to information re-use, in 2010, the Information Commissioner participated in the international consortium managing the LAPSI project (Legal Aspects of Public Sector Information), the purpose of which is to create a thematic network in the field of the re-use of public information. The focus of the project is to reveal and remove legal barriers to accessing and re-using public information in the fields of law, informatics, intellectual property, privacy, and competition-related, administrative, and environmental law, as well as the establishment of strategies for overcoming such barriers.



3 ACTIVITIES IN THE FIELD OF PERSONAL DATA PROTECTION

3.1. The concept of personal data protection in the Republic of Slovenia

The concept of personal data protection in the Republic of Slovenia is based on the provisions of Article 38 of the Constitution of the Republic of Slovenia, according to which, personal data protection in the state is one of the constitutionally guaranteed human rights and fundamental freedoms. The provision of Article 38 of the Constitution of the Republic of Slovenia ensures the protection of personal data and prohibits the use of such data in a manner contrary to purpose for which it was collected; furthermore, everyone has the right to access the collected personal data that relates to him, and the right to judicial protection in the event of any abuse of such data. Of particular importance to the normative regulation of personal data protection is the second paragraph of Article 38 of the Constitution of the Republic of Slovenia, which determines that the collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided by law (general, organic laws and sectoral laws). This entails a so-called "processing model" with determined rules regulating permissible processing of personal data on a legislative level. In accordance with this model, in the field of personal data processing everything is prohibited except that which the law explicitly allows – and in the private sector also only with the explicit consent of the individual concerned. Each instance of personal data processing entails an interference with the individual's constitutional right to personal data protection. Thus such interference is allowed only if the law explicitly specifies exactly what personal data may be processed; additionally, the purpose of processing the personal data must be clearly determined, and adequate protection and security of the personal data must be ensured. The purpose of processing the personal data must be constitutionally admissible, while only the personal data that are appropriate and strictly necessary to realise the legally defined and constitutionally admissible purpose may be processed.

The Personal Data Protection Act[12] was adopted by the National Assembly of the Republic of Slovenia on 15 July 2004, and has been in force since 1 January 2005. The adoption of this Act was primarily necessary due to the accession of the Republic of Slovenia to the European Union, and the resulting obligation to harmonise personal data protection with the provisions of Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[13].

In July 2007, amendments to the Personal Data Protection Act were adopted by means of the Act Amending the Personal Data Protection Act[14]. This legislation introduced two important novelties, namely from the perspective of the administrative – and as a consequence thereof, also the financial – disburdening of data controllers, and the regulation of certain methods easing the manner in which individuals may access their own personal data. The amendments significantly narrowed the circle of data controllers obligated to enter personal data filing systems into the register, and also brought a number of positive solutions, in particular, relief for individuals to whom certain personal data relate. The consolidated Personal Data Protection Act[15] (hereinafter: PDPA-1) was published in September 2007.

[12] Zakon o varstvu osebnih podatkov, Official Gazette RS, No. 86/2004.

[13] Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, No. L 281, 23 November 1995.

[14] Zakon o spremembah in dopolnitvah zakona o varstvu osebnih podatkov, Official Gazette RS, No. 67/2007.

[15] See supra note 4.

3.2. A Review of Activities in the Field of Personal Data Protection in 2010

In 2010, the Information Commissioner conducted 599 cases due to suspected violations of PDPA-1 provisions, of which 202 were in relation to the public sector and 397 to the private sector. Against public sector legal entities 176 complaints were filed and 26 procedures were initiated ex officio, whereas 367 complaints were filed and 30 procedures initiated ex officio with regard to the private sector. In comparison to the statistical data for 2009, the number of cases related to suspected violations of the PDPA-1 remained at almost the same level. Upon the examination of complaints received and due to ex officio procedures, 150 inspection procedures were initiated against public sector legal entities and 306 against legal entities in the private sector. Within the framework of inspection procedures, 267 physical inspections were carried out and on the basis of Article 33 of the Inspection Act[16], 54 warnings due to minor irregularities were issued orally and accordingly logged in the official records. Furthermore, 85 administrative decisions were issued, whereby the liable entities were ordered to undertake certain measures in order to eliminate the established irregularities. In 2010, 482 inspection procedures were concluded, of which 229 had been initiated before 2010.

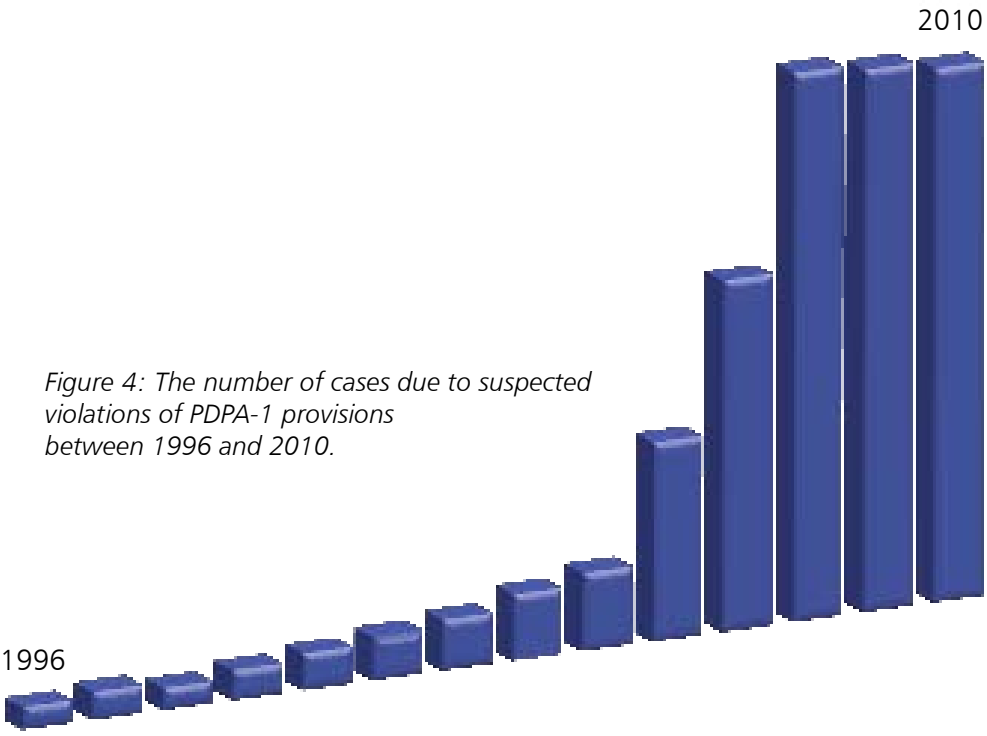


Figure 4: The number of cases due to suspected violations of PDPA-1 provisions between 1996 and 2010.

The largest number of suspected violations of PDPA-1 provisions related to the following:

- Unlawfully collecting or requiring personal data (102 cases);
- transfer of personal data to unauthorised users by the data controller (101 cases);
- unlawful publication of personal data, e.g. on notice boards or in the media (90 cases);
- abuse of personal data for direct marketing purposes (86 cases);
- unlawful video surveillance (59 cases);

[16] Zakon o inšpekcijskem nadzoru, Official Gazette RS, No. 43/2007 – official consolidated text.

- inadequate security of personal data (47 cases);
- other, e.g. unlawful implementation of biometric measures, the processing of personal data in a manner contrary to the purpose for which such was collected (58 cases).

Figure 5: The number of cases due to suspected violations of PDPA-1 provisions between 2006 and 2010.

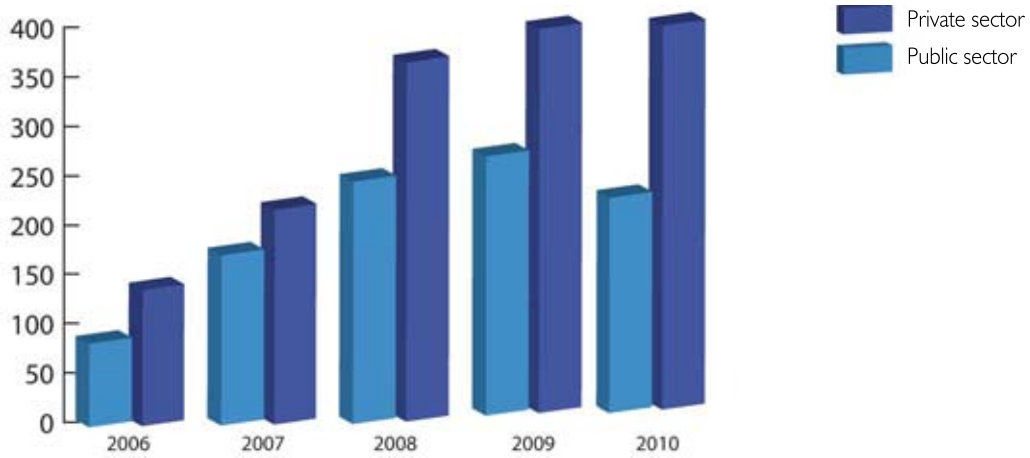
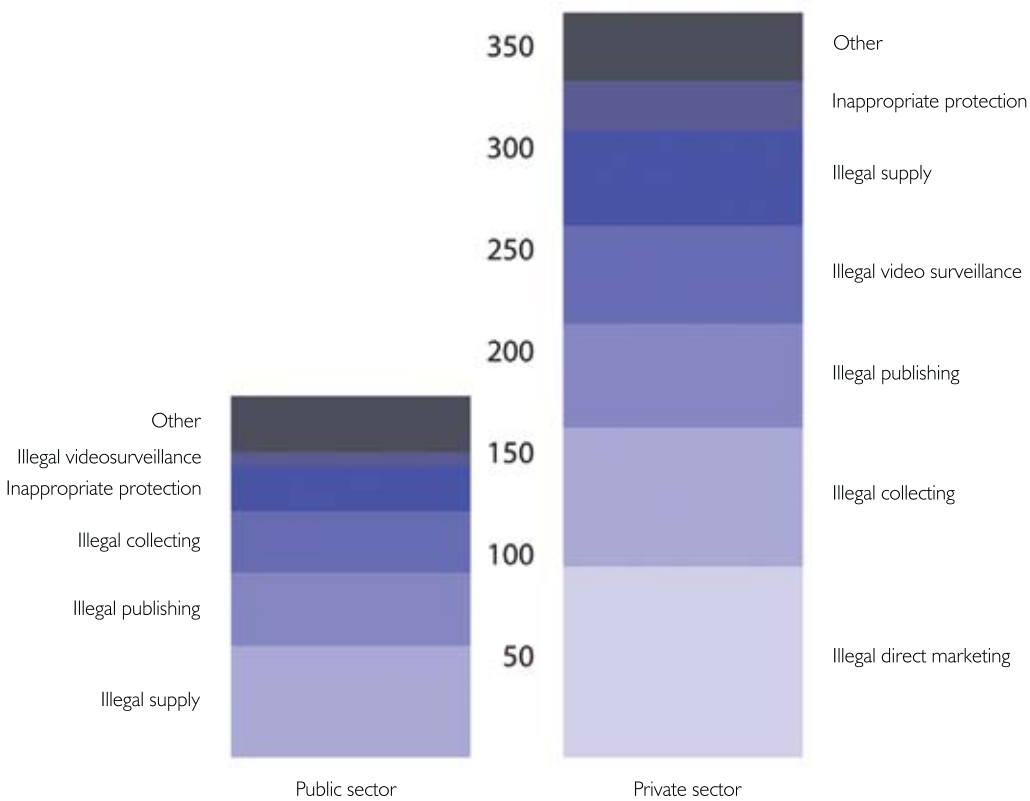
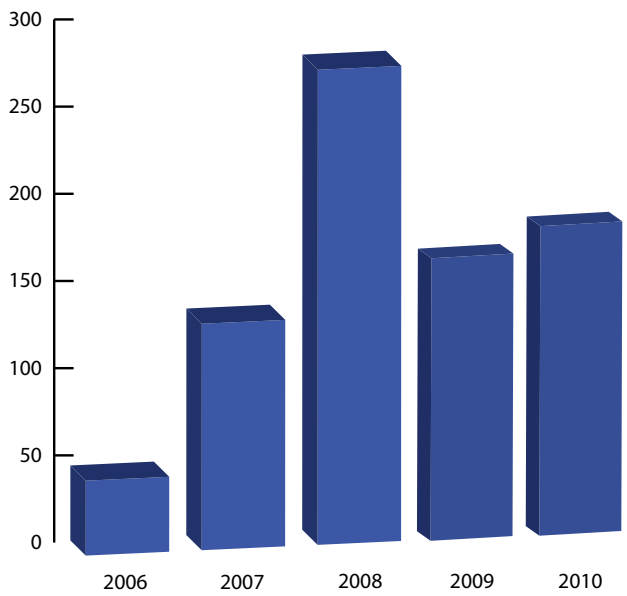


Figure 6: Complaints regarding unlawful processing of personal data in 2010 – a comparison between the public and the private sectors.



In 2010, 179 offence procedures were initiated, 45 procedures against public sector legal entities, 82 procedures against private sector legal entities, and 52 procedures against individuals.

Figure 7: The number of offence procedures initiated between 2006 and 2010.



In 2010, the Information Commissioner issued the following in relation to offence procedures:

- 36 warnings (6 in relation to procedures initiated in 2009)
- 116 decisions regarding violations (i.e. 81 cautions, of which 19 were in relation to procedures initiated in 2009; and 35 fines, of which 8 were in relation to procedures initiated in 2009)
- 10 penalty notices.

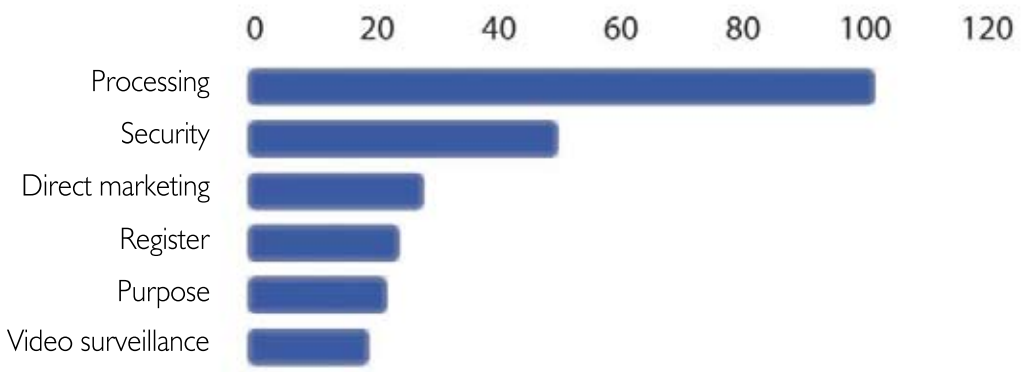
For reasons of efficiency, the Information Commissioner issued 87 warnings for minor offences on the basis of Article 53 of the Minor Offences Act (of which 30 were in relation to inspection procedures initiated in 2009 or 2008).

Violations (one procedure may entail several violations) occurred in relation to the following:

- personal data processing: Article 8 of the PDPA-1 (103 cases);
- security of personal data: Articles 24 and 25 of the PDPA-1 (51 cases);
- direct marketing: Articles 72 and 73 of the PDPA-1 (29 cases);
- the establishment of filing system catalogues and supply of the data to the Register of Filing Systems : Articles 26 and 27 of the PDPA-1 (25 cases);
- the collection and further processing of personal data: Article 16 of the PDPA-1 (23 cases);
- video surveillance: Articles 74 through 77 of the PDPA-a (20 cases);
- security of sensitive personal data: Article 14 of the PDPA-1 (19 cases);
- contractual data processing: Article 11 of the PDPA-a (16 cases);
- not undertaking measures imposed in inspection procedures; violations of the provisions of the Inspection Act (11 cases);

- data retention period: Article 21 of the PDPA-1 (6 cases);
- traceability of the supply of personal data: the third paragraph of Article 22 of the PDPA-1 (4 cases);
- processing of sensitive personal data: Article 13 of the PDPA-1 (3 cases);
- informing individuals on personal data processing: Article 19 of the PDPA-1 (3 cases);
- photocopying identity cards and passports: Article 3.a of the Identity Card Act and Article 4.a of the Act on the Passports of the Citizens of the Republic of Slovenia (3 cases);
- the implementation of biometric measures: Articles 78 through 81 of the PDPA-1 (3 cases).

Figure 8: The most common violations of PDPA-1 provisions in 2010.



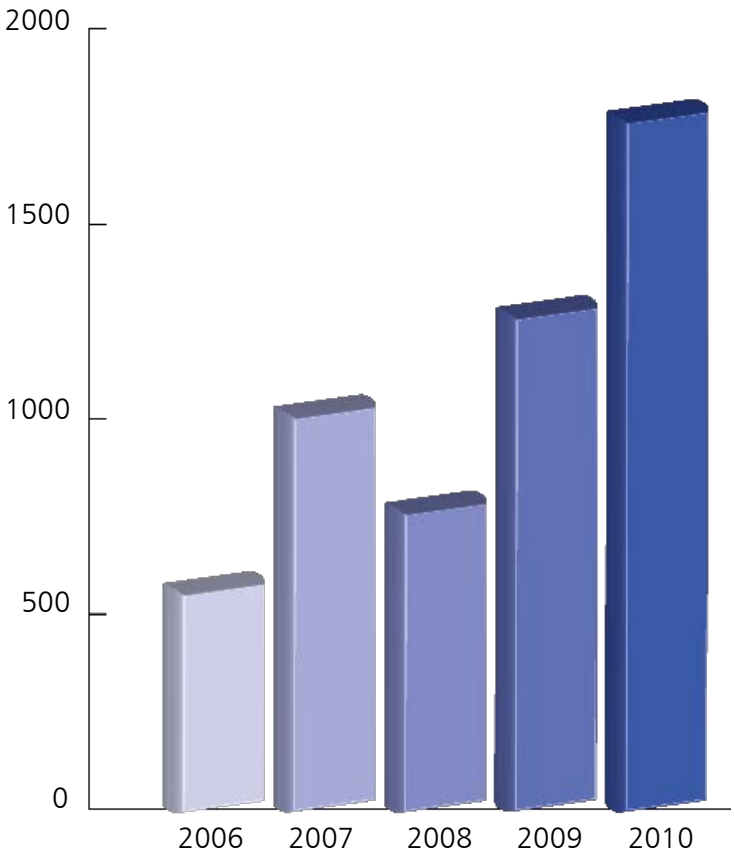
Violators filed 19 requests for judicial protection against the decisions issued, of which 15 were against fines and 4 against cautions.

In 2010 the Information Commissioner received 15 judgments whereby local courts decided on requests submitted for judicial protection against decisions issued in previous years by the Information Commissioner regarding offences, as follows:

- the request for judicial protection was dismissed as unfounded while the decision of the Information Commissioner was upheld (11 cases);
- the request for judicial protection was granted, resulting in the decision of the Information Commissioner being annulled and the offence procedure stayed (3 cases);
- • the request for judicial protection was granted to the extent that it referred to the sanction pronounced, resulting in the sanction being changed; otherwise, the request for judicial protection was dismissed as unfounded (1 case).

In 2010 the Information Commissioner received 1,859 requests to issue a written explanation or an opinion in relation to specific questions, which is a significantly higher number than the 1,334 requests received in 2009. Requests for an opinion or an explanation are becoming more demanding in terms of content since the public is increasingly more familiar with the PDPA-1 and the rights of individuals pursuant to it. With regard to more demanding questions or questions that it had not responded to before, the Information Commissioner issued 575 written opinions and explanations, whereas it referred individuals asking questions it had previously answered to the already formulated opinions referring to such; it issued 1,284 such referrals and recommendations related to the PDPA-1. Furthermore, the Information Commissioner issued opinions and explanations orally – everyday between 9 a.m. and 3.30 p.m. an officer on duty is available at the office of the Information Commissioner who can answer questions over the telephone.

Figure 9: The number of requests for an opinion between 2006 and 2010.



In 2007 the Information Commissioner received 40 applications regarding the introduction of biometric measures, in 2008 it received 16 such applications, 10 applications in 2009, and only 6 in 2010, which shows a constant decrease in the number thereof. In 2010 it issued 8 decisions on the permissibility of implementing such measures, of which 4 were in relation to applications received in 2009. In 5 cases such implementation was granted, in 2 cases it was rejected, and in one case the applicant's request was partially granted.

Positive decisions were issued to legal entities with regard to whom it was established that the implementation of biometric measures was necessary for them to carry out their activities, ensure the security of people or property, or ensure the security of confidential information or business secrets. In order to safeguard property and people, the Information Commissioner permitted a bank to implement biometric measures entailing scanning the irises of employees who enter its vaults at three locations in Slovenia. Furthermore, it permitted an applicant consulting on computer devices and software applications to implement biometric measures by installing a Smarti® DIADEM system, for the purpose of controlling access to the control room. An applicant whose activities include operating web portals was permitted to implement the biometric measure of scanning the fingerprints of employees who, due to the nature of their work and tasks, need to enter thirteen rooms owned by a telecommunications operator. Applicants whose registered activities concern line-based telecommunications and electricity production were also granted requests and permitted to implement biometric measures for the purpose of controlling access to a telecommunications area and a high-security control area by means of fingerprint scanners. The Information Commissioner partially granted a request by a casino and permitted the implementation of biometric measures for the purpose of carrying out operations and the safeguarding of property by means of taking fingerprints of the employees entering the

following rooms at the applicant's headquarters: the cash room, the audio and video room, the counting room, the vault, and the control room. The applicant may apply biometric measures for the purpose of monitoring working hours only by performing simultaneous biometric supervision of access to specific rooms and working hours. In the procedure it was established that at any given moment a clearly specified number of employees must be present on the premises and at specific work posts, and that by applying more lenient measures the applicant would not be able to ensure a precise and constantly up-to-date record of presence. Decisions rejecting requests were issued to two applicants whose stated intention was to introduce biometric measures for the purpose of monitoring working hours, i.e. the presence of employees at their work posts, primarily because such measures are more practical than a system employing proximity ID cards or because they would like to prevent the abuse of the latter by people borrowing such cards from one another. On the basis of such reasons it is not possible to grant the implementation of biometric measures since such would entail an excessive and non-essential interference with employees' privacy, as it is possible to record presence in a less intrusive manner.

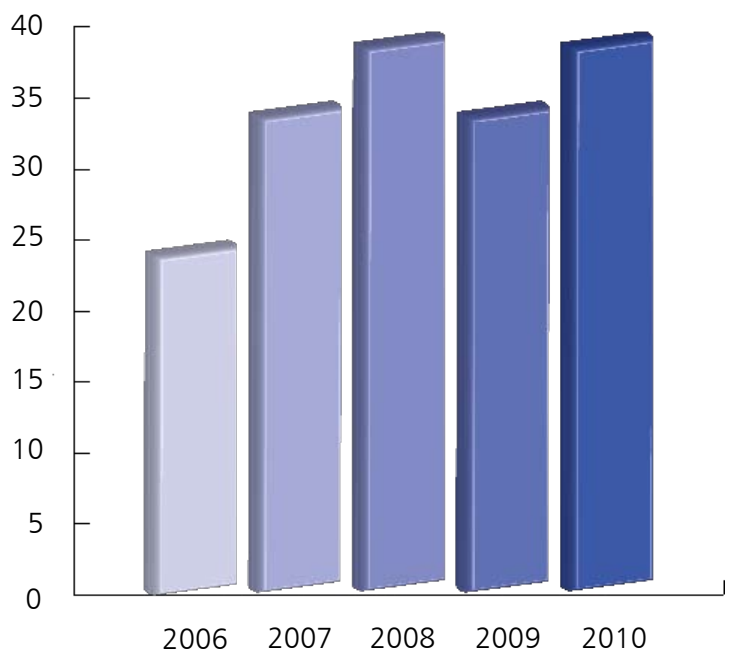
In 2010, the Information Commissioner received eight applications for authorization of transfer of personal data to third countries. It issued ten decisions, of which two were in relation to applications received in 2009. All applicants who received decisions were permitted to transfer personal data:

- The Information Commissioner permitted a company operating in the field of market and public opinion research to transfer personal data pertaining to its employees to the USA for the purpose of centralising administration in order to raise efficiency, facilitate the management of internal occupational resources and the assessment of employee efficiency, and supervise employees, as well as for other activities related to human resource management.
- The Information Commissioner permitted a wholesaler of pharmaceuticals and medicinal aids and materials (the data exporter) to transfer and supply personal data pertaining to its employees and clients to its contractual data processor in the USA for the purpose of keeping records on business expenses and trips by means of an on-line service.
- The Information Commissioner permitted a company operating in the field of telecommunications (the data exporter) to transfer and supply to the subsidiaries of the group, who were signatories to the company's Internal Contract on Data Transfer, personal data pertaining to the following groups: the employees of the data exporter, contractors working on its behalf, candidates for employment at the data exporter, employees and appointed representatives of clients and users of the services of the data exporter, and employees and appointed representatives of suppliers of goods and services that the data exporter purchases for the purpose of human resource management and for providing clients with services purchased.
- The Information Commissioner permitted four companies of a group involved in wholesaling pharmaceuticals and medicinal aids and preparations and in the production of pharmaceutical preparations (the data exporters), to transfer and supply – upon receiving decisions (each data exporter received its own) – to their contractual data processor in India personal data pertaining to their employees and to third parties whose personal data may appear in communication exchanged by means of software applications regarding which the data importer is to ensure support. The data importer will provide the data exporters services related to application management and detecting and solving problems related to e-mail and Lotus Notes data files.
- The Information Commissioner permitted a company involved in pharmaceutical marketing (the data exporter) to transfer and supply to its contractual data processor in Turkey personal data pertaining to its employees, consultants, and agents and to the employees, consultants, and agents of its clients. The purpose of the data transfer is to enable the performance of tasks related to the examination of the business operations of the company, primarily the compilation of statistical reports which are based on data regarding the sales of individual pharmacies and which show activities according to particular regions.
- The Information Commissioner permitted a company involved in pharmaceutical

marketing (the data exporter) to transfer and supply to its contractual data processor in the USA personal data pertaining to its employees, consultants, and agents and to the employees, consultants, and agents of its clients. The data is to be transferred for the purpose of storage in the IMS group central register, the performance of tasks related to human resources, making salary payments, and contacting the company's consultants and agents for the purpose of carrying out the company's operations.

- A pharmaceutical company proposed that the Information Commissioner issues a decision stating that, to the extent that such refers to the transfer of data to organisations operating in accordance with the safe harbour privacy principles implemented in accordance with the FAQ thereof, the USA ensures an appropriate level of personal data protection. In the examination of the application the Information Commissioner established that the USA is not on the list determined in Article 66 of the PDPA-1, and furthermore, that on 26 July 2000 the European Commission had already issued Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), in accordance with which the safe harbour privacy principles ensure an appropriate level of protection of personal data transferred out of the European Community to organisations based in the USA. The Information Commissioner concluded that the USA ensures an appropriate level of protection of personal data to the extent that such concerns the transfer of personal data to organisations operating in accordance with the safe harbour privacy principles.

Figure 10: The number of applications for authorisation of transfer of personal data to third countries between 2006 and 2010.

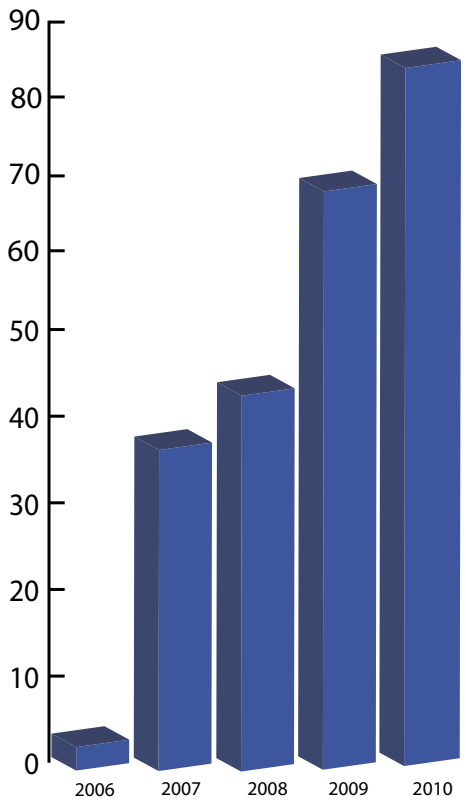


In 2010, the Information Commissioner received nine applications requesting permission regarding linking personal data filing systems. It issued seven decisions, of which one was in relation to an application received in 2009, whereby it granted data controllers permission to link their filing system with one or more filing systems (e.g. [n.b. unofficial translations of the names of some Slovene institutions] a direct link between the register of current accounts, the central population register, the tax register, and the business

register of Slovenia; a direct link between the tax register, the record of written customs declarations, the record of customs permits issued, the record of excise duty registrants and small producers of wine and spirits, the record of entities entitled to the return of excise duty, the register of tax representatives, unauthorised recipients and persons filing reports on individual business transactions, the record of collected taxes, the record of instruments submitted for securing the payment of taxes, and the record of entities subject to the payment of the environmental tax; the e-VEM information system is linked to the filing system on foreigners; a direct link between the central record of recipients of subsidised school meals, the child benefit record, and the central population register; the following are linked within the framework of the e-Rojstva (e-Births) application: basic medical records, the central population register, and the register of births, marriages, and deaths; a direct link between the record of documentary materials and the central population register; the establishment of a direct link between the register of insured persons, the register of persons entitled to rights following from pension and disability insurance, and the central population register). An individual's EMŠO number (unique personal identity number) or tax number is used as a linking element, while which personal data may be linked and exchanged is determined by law.

In 2010 the Information Commissioner received 85 appeals (in comparison to 48 in 2008 and 70 in 2009) concerning the right to access one's personal data, which shows an increase in the number of appeals. Appeal procedures concerning access to one's personal data included appeals in cases when individuals did not manage to obtain medical records under the Patients Rights Act. In 2009 the Information Commissioner received eight and in 2010 four such appeals. The Information Commissioner noted a decrease in the number of cases due to the non-responsiveness of personal data controllers, i.e. data controllers who do not respond in any manner to individuals' requests related to accessing their own personal data. In 2009 the number of appeals due to non-responsiveness amounted to 51% and in 2010 38% of all appeals concerning requests to access one's own personal data. The largest share of appeals against decisions refusing a request to access one's own personal data concerned state authorities, ministries, and constituent bodies (31 cases). In 14 cases applicants addressed their requests to access their own personal data to their employers who subsequently refused such. Of all applications received, 58 were resolved in 2010. In 23 cases data controllers provided information immediately after the Information Commissioner called on them to do so, 13 data controllers were ordered by a decision to enable applicants to access their own personal data. One data controller filed an appeal with the Administrative Court against the decision of the Information Commissioner, while in three cases appellants initiated administrative disputes regarding the decision of the Information Commissioner dismissing their appeal.

Figure 11: The number of appeals regarding the right to access one's personal data between 2006 and 2010.



3.3. The Most Significant Cases Involving a Violation of the Personal Data Protection Act

Processing of the personal data of users of the Urbana travel card

In an inspection procedure conducted with regard to the public transportation company Ljubljanski potniški promet (hereinafter: LPP), the Information Commissioner determined that for all passengers who paid the fare by means of the Urbana personalised electronic travel card, the company was collecting and retaining data on the time and place of entering a bus and the bus line taken (location data), although it did not have a legal basis to process such data of passengers paying the fare with a personalised non-transferrable fixed-period travel card (hereinafter: personalised travel card).

On the basis of the decision of the Information Commissioner, LPP had to cease collecting such data and was obliged to delete the location data of all such passengers who had used or paid the fare with a personalised travel card. In the inspection procedure the Information Commissioner determined that the processing of personal data occurred only with regard to the green Urbana card, which is personalised and non-transferable. When a green Urbana card is used, LPP, among other data, processes the location data of the card user, for which there is neither a basis in the law nor in any personal consent granted; furthermore, the processing of these data was not necessary for the fulfilment of the contract between the passenger and the transportation company. Namely, by buying or obtaining this personalised travel card, the user gains the right to an unlimited number of journeys on all lines of the city transportation system for a fixed or unlimited period of time, and thus collecting data on the time and place of entering a bus and on the bus line taken is completely unnecessary. The Information Commissioner also assessed that processing location data in order to monitor the traffic flow is also unnecessary. For such purpose LPP only needs data on the number of passengers riding on individual lines at specific times or the number of passengers entering buses on specific bus lines at specific times at specific bus stops, and not data on which passengers were transported or entered a bus. In its decision the Information Commissioner ordered LPP to adjust the functioning of the devices by means of which passengers validate their Urbana travel cards upon entering a bus such that the devices no longer display data on the type of fixed-period travel card used (e.g. for retired persons, students, etc.) as any random passenger entering the bus can view such data on an individual passenger validating their card. In the procedure it was namely established that data on the type of personalised fixed-period travel card is personal data which is retained in the personal data filing system of LPP and that revealing such data to random other passengers entails inappropriate security of such data.

Telephone numbers as personal data and banning the use of personal data for the purposes of direct marketing

The Information Commissioner carried out an inspection following a complaint in which the complainant claimed that an individual joined a certain SMS club with her specific telephone number in 2007 and then also immediately cancelled her membership in the SMS club. Two years later she received an advertising message by SMS from which it was evident that it was connected to her membership in the SMS club. The company operating the SMS club argued that a telephone number cannot be treated as the personal data of an individual, and that it was further specified in the general conditions of the club that the personal data required of the individual would no longer be processed only seven years after the cancellation of membership.

In the inspection procedure the Information Commissioner established that a telephone number is personal data and that for deciding whether a person is identifiable or not it is necessary to consider all the means to identify such person that can be expected to be used

by either the data controller or any other person. In assessing if an individual is identifiable it is necessary to also consider the time component, as due to technological advances it is possible to use ever more means of identification. To what degree certain data are sufficient for identifying an individual depends on the circumstances in the specific situation. It is necessary to interpret the definition of personal data broadly and a telephone number can also be deemed to be personal data if it is possible to identify such person thereby. The Information Commissioner also established that with the provisions of the general conditions of the SMS club the company violated the intent of the provision of Article 73 of the PDPA-1, according to which a data controller is obliged to prevent further use of personal data for the purposes of direct marketing within 15 days if the individual at issue so requests. Therefore, the Information Commissioner issued a decision by which it ordered the company to delete the phone number of the individual and to delete the text in the general conditions of the club which refer to cancellation of its commercial services. The company appealed the decision before the Administrative Court. In its judgment the Administrative Court upheld the decision of the Information Commissioner that a telephone number is personal data and that it is not relevant whether it is accompanied by other personal data. It furthermore decided that companies carrying out direct marketing may not retain personal data after the person to whom it refers has cancelled use of their services.

Carrying GPS monitoring devices by newspaper distributors

The Information Commissioner conducted an inspection procedure of a company which is involved in the publication and distribution of newspapers due to the suspicion of illegal collection of personal data by means of GPS monitoring devices. The company gave employees delivering newspapers GPS monitoring devices and required them to carry such device in the pocket of their work uniform while delivering newspapers, magazines, and advertisements. In the event that they did not carry the monitoring device, the employee was threatened with immediate termination. The Information Commissioner issued the company a decision ordering it to cease collecting the personal data of employees delivering newspapers by means of the GPS monitoring devices and to destroy the personal data of the employees delivering newspapers which it had collected by means of the GPS monitoring devices up to the issuance of the decision.

The Information Commissioner established that such supervision or monitoring of the movements of employees delivering newspapers as carried out by the company was inadmissible. In the relationship of parties of unequal strength which the company has with the individuals at issue (its employees delivering newspapers) it is difficult to defend the position that the personal consent of such employees which enabled the company to process their location data was given voluntarily and freely, especially if their job depended on giving such consent, as was the case in this specific instance. The Information Commissioner also concluded that all the purposes for doing so stated by the company could have been achieved by measures that would encroach to lesser degree on the privacy of such employees. If a kidnapping or other criminal offence were to be committed against an employee delivering newspapers or the newspapers were to be stolen, the company should hand the matter over to the competent authority for resolution. The number of newspapers that an individual newspaper delivery person carries and the value thereof are not of such amount that the interference with the privacy of the newspaper delivery person (i.e. the requirement to carry the GPS device) is well-founded or justified. In addition, the car, motorcycle, or other means of transportation used to deliver newspapers are owned by the delivery persons. Furthermore, the company does not urgently need such data in order to determine the location of a newspaper delivery person in the event of a traffic accident, as in such a situation the persons involved in the traffic accident would call the competent authority (i.e. the police). Moreover, the collection of location data is not necessary for establishing the successfulness and timeliness of such deliveries and the speed of resolving customer complaints, as the use of location data in the event a client does not receive a newspaper is not evidence that the delivery person actually delivered it, but only evidence that at a certain time the newspaper delivery person was at a certain place, but not also what he did there.

The collection of personal data when making a purchase with a gift certificate

In an inspection procedure initiated by the Information Commissioner with regard to a retail trading company, it was established that when customers wanted to purchase goods with a gift certificate, the company required them to produce a personal identification document from which the company copied their personal data due to the alleged possibility of counterfeit gift certificates. The Information Commissioner issued a decision by which it ordered the retail trading company to delete the personal data of customers who paid for their purchases with a gift certificate as the processing and collection of the personal data of customers was not proportionate. Furthermore, this case raises doubts as to how freely customers would consent to providing personal data if the retail trading company, as the issuer of the gift certificates, refused to fulfil its obligations arising from the gift certificates in the event the customer does not wish to provide his personal data. With the issuance of the gift certificate the issuer undertakes to fulfil the obligation specified on the voucher. The bearer of the gift certificate exercises the right he is entitled to on the basis of the gift certificate by presenting it to the issuer, whereby the identity of the bearer (his personal data) is not relevant for the obligation to be fulfilled correctly. The Information Commissioner established that the retail trading company as the issuer of the gift certificate may object to the bearer of a gift certificate that the gift certificate is counterfeit, with regard to which the identity of the bearer is not relevant. In practice, this entails that the salesperson would simply check the authenticity of the gift certificate, as authentic gift certificates have certain features which allow them to be recognised. In the event that it is established or suspected that the gift certificate is counterfeit, the salesperson can refuse to allow the bearer to pay with the gift certificate, however the salesperson may not require that the bearer provide personal data.

The use of video surveillance footage contrary to the purpose of the implementation of video surveillance

Recent years have seen a significant increase in the proportion of public space under video surveillance. Very frequently local communities wish to install video cameras in order to monitor squares, parking lots, retractable bollards at the entrance to pedestrian zones, recycling stations, streets, etc. Under the PDPA-1, the legislature limited the use of video surveillance as a form of processing personal data such that there is a closed circle of permissible purposes for which it may be implemented. The Information Commissioner established that ensuring the safety of people and the protection of property are legitimate purposes for which video surveillance may be implemented or for which purpose video surveillance footage of a public space may be stored and viewed, whereas the detection of offences and the provision of evidence thereof with regard to improper rubbish disposal or illegal parking are not legitimate purposes. The operator of a video surveillance system may use such footage in the event protected property is damaged (e.g. rubbish containers, retractable bollards, etc.). The use of video surveillance system footage in order to detect and provide evidence of offences is not in accordance with the purpose for which such footage is stored. Therefore, such use of video surveillance footage is contrary to PDPA-1 and the Constitution.

In an inspection procedure the Information Commissioner determined that a municipality was detecting stationary traffic violations (illegal stopping and parking) by reviewing footage taken by a video surveillance system. Thus it was not necessary for traffic wardens to determine "on the spot" whether the illegally parked or stopped vehicle entailed a violation and obstacle for young parents with baby carriages and persons with disabilities, but could simply review the footage in the office, take down the registration numbers of illegally parked or stopped vehicles, examine the register of motor vehicles in order to identify the driver, and send a parking ticket. In its decision, the Information Commissioner ordered the municipality to cease reviewing footage for the purpose of imposing sanctions

for illegal parking in public spaces. The municipality filed an appeal against the decision before the Administrative Court, which in 2011 upheld the decision of the Information Commissioner.

The forwarding of documents by the court in execution proceedings to the debtor's employer

The Information Commissioner conducted a procedure against a court carrying out enforcement proceedings. It concluded that the court forwarded documents relating to the garnishment of wages of the debtor to her employer, with regard to which it disclosed the personal data of the debtor and her relatives by forwarding the enforcement order and a large number of other documents (the judgement which, as the enforcement instrument, was enclosed with the enforcement proposal, and documents regarding the account from which the basis of the liabilities of the debtor were evident), without a legal basis or the personal consent of the individual, which were not necessary for the enforcement proceedings or for repaying the creditor. The court referred to the public nature of the judicial proceedings and to the publication of the judgment.

In the inspection procedure it was established that when an enforcement order is issued against a debtor, he cannot avoid the fact that his employer, if the garnishment of the debtor's wages is permitted, thereby learns of the judgment of the court issued against him, since, in accordance with the provisions of Article 45 of the Enforcement and Securing of Civil Claims Act[17], the court must serve the enforcement order on the debtors of the debtor. The court does not need to substantiate its decision with the documents that were the basis for the enforcement order since it is simply necessary to believe that the court issued the enforcement order lawfully. The Information Commissioner also established that the judgment is indeed publicly available, but in an anonymised form. The fact that the hearing at the court was open to the public does not, however, entail that also the documents and the personal data in the case file should become public. Irrespective of the public nature of the judicial proceedings (such processing of personal data is determined by the Civil Procedure Act), the court must have a basis in law for forwarding the personal data in the individual case file.

The publication of personal data in the media

In 2010, the Information Commissioner received a considerable number of complaints from individuals against the media or individuals due to the publication of personal data in newspapers and on the internet (e.g. on Facebook, in blogs). In the majority of cases the Information Commissioner informed the complainant that an inspection procedure would not be conducted with regard to their complaint. Not all personal data are automatically subject to protection in accordance with the PDPA-1, rather such enjoy protection only if they are part of a personal data filing system or are intended for inclusion therein. The Information Commissioner, therefore, always first establishes whether the personal data are part of a personal data filing system. If it establishes that they are, it proceeds to establish whether they were published lawfully or not, and in the event of a violation it pronounces the appropriate inspection measures and sanctions. Disclosing information which only entails stating some facts (most often in postings on social networks) which do not comprise personal data from a data filing system, does not entail a violation of the PDPA-1; however, this does not also entail that the injured party does not have the right to possible judicial protection due to an interference with his privacy, in a broader sense, or due to an interference with his personality rights. The individual can exercise legal protection of the broader right to privacy in criminal and civil proceedings before the competent courts.

[17] Zakon o izvršbi in zavarovanju, Official Gazette RS, No. 3/2007 – official consolidated text 4, with amendments.

3.4. Overall Assessment and Recommendations regarding the status of Personal Data Protection

In the field of personal data protection, in 2010 the Information Commissioner noted an increase in the number of questions submitted by natural persons and legal entities regarding personal data protection and a slight increase in the number of appeals due to the refusal of requests to access one's personal data, while the number of requests for opinions, inspection cases, offence cases, and cases in which the Information Commissioner considered the issuance of permits for the implementation of biometric measures, the transfer of personal data to third countries, and the linking of filing systems remained at the same level as in 2009. Thus, in 2010 the Information Commissioner received 1,284 questions in the field of personal data protection (compared to 738 the year before), 575 requests for an opinion (compared to 596 the year before), and initiated 599 inspection procedures (compared to 624 the previous year), 179 offence procedures (compared to 163 the previous year), 85 procedures concerning access to one's personal data (compared to 70 the previous year), 6 cases concerning the issuance of a permit for the implementation of biometric measures (compared to 10 the previous year), 8 cases concerning authorisation of transfer personal data to third countries (compared to 7 the previous year), and 9 cases concerning the issuance of a permit to link filing systems (compared to 5 the previous year).

In considering appeals due to the denial of access to one's personal data, the Information Commissioner established that a significant portion of the appeals (32 of 85 in total in 2010) were filed due to the non-responsiveness of personal data controllers. Upon receiving an individual's request to access his personal data the data controller must, within the period of time determined (within 15 or 30 days at the latest), enable the individual to examine, copy, or photocopy his personal data, or provide him with the requested extract, list of recipients, written certificates, or information and notifications regarding his personal data, or notify him within the same time period why such will not be provided. If the data controller fails to do so, the request is deemed to be refused and the individual may file an appeal due to the non-responsiveness of the data controller with the Information Commissioner. However, with regard to such, it must be noted that the non-responsiveness of data controllers does not entail merely the refusal of an individual's request but also an offence under point 13 of paragraph 1 of Article 91 of the PDPA-1 and therefore in such cases the Information Commissioner initiates an offence procedure against the personal data controller.

In the area of video surveillance, the Information Commissioner established that such is spreading rapidly and can be encountered at practically every step. This field is insufficiently regulated in the currently applicable act and the Information Commissioner has proposed to the Ministry of Justice that the provisions thereof be amended. With regard to irregularities established in relation to the implementation of surveillance, what must primarily be noted is inadequate record keeping regarding reviewing or using video surveillance footage, the use of footage for unlawful purposes, poorly marked and incomplete notification of video surveillance, the non-existence of a written decision of an employer on the implementation of video surveillance, and the non-existence of video surveillance footage filing system catalogues.

In the area of direct marketing, the Information Commissioner established that an increasing number of stores are introducing various loyalty cards, which can be obtained only by supplying certain personal data that is then ever more frequently used, together with information regarding purchases made with such a card, in order to profile customers and for direct marketing purposes. It was established for 2010, similarly as with previous periods, that in direct marketing personal data controllers do not notify individuals of their right to demand, at any point, in writing or some other defined manner, that their personal data no longer be used for direct marketing purposes. Furthermore, it was found

that despite certain individuals clearly prohibiting the use of their personal data for direct marketing, some data controllers continued to use such, and consequently the Information Commissioner initiated offence procedures against them and pronounced appropriate sanctions.

With regard to the implementation of procedures and measures for personal data security determined by Articles 24 and 25 of the PDPA-1, it must be noted that such is often still not at an appropriate level, in some cases due to insufficient finances. Furthermore, formal irregularities can be found as well in instances where personal data controllers do not determine in their internal acts appropriate procedures and measures for personal data protection and do not determine the persons responsible for individual filing systems and the persons who, due to the nature of their work, are allowed to process certain personal data. Some data controllers understand information security too narrowly – either as IT security or as entailing mere technical measures; what is lacking, however, is an integrated approach and appropriate emphasis on organisational measures. Nevertheless, irrespective of all the above-mentioned, it can in general be said that knowledge of legislative requirements and the appropriateness of procedures and measures are increasing. In the future, more emphasis will have to be placed on organisational measures, such as user education, since over time the emphasis usually shifts slowly from technical to organisational measures. By means of the latter, data controllers attempt to analyse risks and envisage forms of social engineering. Furthermore, emphasis is also placed on appropriate selection and management of passwords, and similar.

With regard to the implementation of procedures and measures for personal data protection, attention should also be called to the disclosure of e-mail addresses when sending e-mail messages. In 2010, the Information Commissioner considered a number of cases in which data controllers sending group e-mails disclosed the e-mail addresses of the addressees to all recipients, who, however, were not entitled to such data. Such a disclosure occurs, for example, when an employer sends all applicants for an open position an e-mail telling them that they were not selected, whereby he enters all addresses in the "To" or "Cc" fields, such that all the e-mail recipients can see, although they are not entitled to, the addresses of the other non-selected candidates, which entails a violation of Articles 8 and 24 of the PDPA-1. Direct marketers can thus, if careless, disclose the database of all their 'clients', i.e. recipients of advertising messages. Therefore, the Information Commissioner calls attention to the fact that in such and similar cases e-mail addresses must be entered in the "Bcc" field (concealed copy), which ensures that recipients do not see the e-mail addresses of other recipients of a certain message.

In 2010 the Information Commissioner paid a great deal of attention also to the question of the expected privacy of employees at the workplace and related problems concerning the use of GPS monitoring devices, work-related e-mail, work telephones, and computers that employees use to a limited extent also for private purposes. Such use undoubtedly causes a conflict between the interests of employers, who have the right to control equipment they own and to monitor to a certain extent that such is used in accordance with the purpose for which it was given to employees, and the interests of employees, who have a well-founded basis to expect a certain degree of privacy and confidentiality at the workplace. Since handling such cases has revealed the pressing problem of the field of workplace privacy being legally inadequately regulated, the Information Commissioner has already called attention to such a number of times. In 2009, it prepared a draft act on communication privacy at the workplace, however the competent ministries have not yet considered it.

In 2010 the Information Commissioner continued its preventative work and dedicated a great deal of attention to continuing to disseminate tools and aids for raising awareness. Guidelines were devised for data controllers regarding how to fulfil the PDPA-1 requirements in practice. The legal basis for issuing such guidelines is provided to Information Commissioner in Article 49 of the PDPA-1, which determines that the Information Commissioner issues non-binding opinions, explanations, and standpoints

regarding questions related to personal data protection and publishes such on its website or in another appropriate manner, and prepares and issues non-binding instructions and recommendations regarding the protection of personal data in individual fields. In 2010 the Commissioner issued the following guidelines in Slovene:

- Guidelines for Personal Data Protection in Online Forums
- Privacy Impact Assessments
- Guidelines for Health Care Service Providers
- Guidelines for the Development of Information Solutions.

In addition to the above mentioned guidelines in Slovene, the Information Commissioner issued the following guidelines in English, accessible on its website:

- Privacy Impact Assessment in e-Government Projects
- Guidelines for Preventing Identity Theft
- Guidelines Regarding Digital Television and Privacy Protection.

Special attention was paid to privacy impact assessments and the promotion of the "Privacy by Design" concept. The Information Commissioner participated in privacy impact assessments in relation to projects involving personal data processing and in planning proposed amendments to legislation. Some of the more interesting projects included ones involving the transition to the implementation of electronic billing, biometric measures, the planned introduction of average speed cameras on the roads and the implementation of Security Information and Event Management tools. Generally, the expert assistance of the Information Commissioner made it easier for liable entities to promptly identify certain risks regarding personal data processing, and to adapt the range of data processed and protection mechanisms accordingly, and thus avoided violations of legislation and high costs.

Furthermore, in 2010 the Information Commissioner participated in the inter-sectoral working groups in the eUprava (e-Government) framework regarding the following projects: eZdravje (e-Health), eSociala (e-Social Services), the eVEM business portal, eArhiviranje (e-Archives), and in an inter-sectoral group for the preparation of the information society developmental document for 2011–2015.

The development of information communication technologies requires the special attention of the Information Commissioner. Some trends in the field of privacy in the information society are especially worrisome, therefore the Information Commissioner monitors them closely. Such include so-called cloud computing, which entails computation, software, storage, and data access services which, from the perspective of final users, do not require a particular physical location or the end user to configure the system that provides such services. An essential characteristic of cloud computing is that data processing does not happen at a static location determined in advance, which is why public forms of cloud computing especially raise serious concerns regarding personal data protection particularly in the field of contractual processing of personal data, personal data security, and transferring data to third countries. In order for cloud computing to be legally and practically acceptable with regard to service providers which are not monitored directly, trust in such services is essential.

Similar holds true for the so-called 'Internet of Things'. An increasing number of devices that we use daily employ the capabilities of information and communication technologies for purposes of data collection, storage, provision, and processing. Such devices lead to activities that people had been able to do anonymously in the past now resulting in personal data processing. These phenomena include intelligent transport systems comprising infrastructure, connections, and devices for controlling traffic flows, danger notifications, and in the event of accidents, establishing the location of vehicles, measuring the behaviour of vehicles and drivers, etc. The use of RFID chips can be classified as such as well, and they are slowly but steadily making their way from the field of logistics into the

retail area and thus raise issues regarding the possibility to monitor the sales of products by means of such, the use of such data for targeted marketing, and the transfer of such data to third parties. Related phenomena where older systems are replaced or upgraded with systems that enable better, faster, and more extensive processing of personal data can be seen also in the field of video surveillance. In the opinion of the Information Commissioner, an increase can be expected soon in the number of video surveillance systems which enable the recognition of individuals from footage. Facial recognition technologies are progressing rapidly and enable the identification of individuals and the automatic recognition of certain parameters, such as age, gender, movement in a monitored area, time spent in particular areas, and similar. Such possibilities have already drawn the interest of various potential users, ranging from stores to prosecution authorities.

As has already been mentioned in previous annual reports, the legal framework has difficulty keeping pace with rapidly developing technologies, which makes certain preventative mechanisms such as privacy impact assessments and consideration of the Privacy by Design concept even more important since it is often impossible to address new services and technologies within the existing legal frameworks. In light of this, what should also be mentioned are the expected amendments to EU Directive 95/46 on protection of personal data – in the process of preparing expert opinions the Information Commissioner was a member of the Article 29 Working Party – which will give greater emphasis to the Privacy by Design concept. In the future, investing in privacy should no longer be perceived as an expense; to the contrary, the absence of timely investments in mechanisms for the protection of privacy will be an indicator of inadequate respect for legislation and thus an expense in itself.


LENS 5x OPTICAL ZOOM

4 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

4.1. Participation in the preparation of laws and other regulations

In accordance with the provision of Article 48 of the PDPA-1, the Information Commissioner issues prior opinions to ministries, the National Assembly, self-governing local community bodies, other state bodies, and bearers of public authority regarding the compliance of the provisions of draft laws and other regulations with the acts and other regulations regulating personal data. In 2010, the Information Commissioner participated in the preparation of 51 laws and other regulations.

4.2. Relations with the public

Throughout 2010, the Information Commissioner provided for the public nature of its work and 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, etc.) and through its website. The Information Commissioner endeavoured to ensure that its website (www.ip-rs.si) was up to date and comprehensive.

Once again the Information Commissioner marked European Personal Data Protection Day on 28 January 2010 and prepared an event intended to draw attention to direct and targeted marketing, which are increasingly encroaching on the privacy of consumers. The central activity of the event was a round table on the theme of Consumer Rights Protection and the Processing of Personal Data for Direct Marketing Purposes. At the round table, stimulating participants from the Slovene Consumers' Association, the large retailer Mercator, the pharmacy chain Lekarne Ljubljana, Združenje za direktni marketing (the Direct Marketing Association), and the Information Commissioner shared opinions and views on direct marketing and the related issues concerning consumers' personal data protection. The Information Commissioner presented awards for good practice in the field of personal data protection in 2009 to data controllers in both the public and private sectors. The Information Commissioner bestowed special recognition on companies that were certified in accordance with the ISO/IEC 27001 Information Security Management System Standard in 2009 and thereby demonstrated a high level of personal data security.

For the eighth year the Information Commissioner marked the International Right to Know Day on 28 September 2010, celebrated since 2002 when a variety of civil society associations from a number states joined together in the Freedom of Information Advocates Network (FOIAnet). On this day, the Information Commissioner and the Ministry of Public Administration organised a joint working meeting whose objective was to analyse the status of this area and formulate common standpoints for further work. It was established that every year there is an increase in the number of applications requesting access to public information, which entails an ever greater awareness of civil society regarding the human right to access public information and concurrently that the purpose of the relevant act is being realised. The number of complaints and appeals in connection with access to public information is also rising. It was also found that public sector authorities are still devoting too little attention to so-called proactive provision of public information. Therefore, liable entities were encouraged in this area to make greater efforts to publish freely accessible information on the internet or in some other suitable manner.

The Information Commissioner provided for the continuing education of liable entities and persons by organising a variety of workshops and seminars; furthermore, the Information Commissioner participated in a number of conferences, workshops, and round tables.

In 2010, the Information Commissioner issued two brochures (in Slovene):

- How to handle patient data and whom to provide it to;
- A brochure on personal data protection intended for consumers.

The Public Opinion and Mass Communication Research Centre carried out research within the framework of the Politbarometer part of the Public Opinion Research on the Relationship of the Public to Current Circumstances and Events in Slovenia Project. The research was carried out in January, May, October, and December, and included an assessment of the public's level of trust in institutions. The January measurement ranked the Information Commissioner quite high, in third place out of twenty-five institutions ranked by the research, namely behind the fire brigade and personal medical doctors, and ahead of, e.g., the euro, the Army, the Human Rights Ombudsman, the President of the Republic, the Police, the European Union, the Commission for the Prevention of Corruption, the Bank of Slovenia, and the Constitutional Court. In the May research, the Information Commissioner rose to second place out of twenty-five. An important part of the research concerns the expression of trust in supervisory institutions, which, in addition to the Information Commissioner, in May included the Human Rights Ombudsman, the Commission for the Prevention of Corruption, the State Prosecutor General, the Director General of the Police, and the Medical Chamber of Slovenia. Of the listed institutions, the Information Commissioner is the highest ranked and those surveyed expressed the highest level of trust in it. The research carried out in October and December found the same. All the mentioned results demonstrate a very firm level of trust in the Information Commissioner.

4.3. International cooperation

In 2010, Information Commissioner employees participated in 19 international seminars and conferences, at 10 of which they also presented their own papers.

As the national supervisory authority for the protection of personal data, the Information Commissioner cooperates with the competent bodies of the EU and the Council of Europe engaged in personal data protection. Cooperation at the international level and participation in the legislative procedures of the EU are also provided for in the European Data Protection Directive (95/46/EC).

In 2010, the Information Commissioner actively participated in five working bodies of the EU which are engaged in supervision of the implementation of personal data protection within individual spheres of the European Union, namely:

- the Working Party for the protection of personal data under Article 29 of the European Data Protection Directive (95/46/EC);
- the Joint Supervisory Body of Europol;
- the Joint Supervisory Authority for Schengen;
- the Joint Supervisory Authority for Customs;
- co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national authorities for the protection of personal data (EURODAC).

The Article 29 Data Protection Working Party adopted a number of important opinions last year, including on the terms "controller" and "processor", online behavioural advertising, on the European code of conduct of the Federation of European Direct and Interactive Marketing (FEDMA) for the use of personal data in direct marketing, on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for radio frequency identification (RFID) Applications, and on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries.

Within the framework of the Article 29 Data Protection Working Party, the Information Commissioner also actively participated in two sub-groups, namely the Internet and Information Technology Sub-Group (the so-called Technology Sub-Group or TS) and the Future of Privacy Sub-Group. In 2010, the former dealt primarily with online social networks, search engines, interactive online maps, behavioural advertising, RFID devices, smart telephones which are capable of transmitting ones geographical location, the practice of collecting data from wireless networks, and the obligations of data controllers in the event of unauthorised access to the personal data they process, as envisaged in the amended Directive EC/2002/58. The Technology Sub-Group prepared many documents, the most important of which is Opinion 2/2010 on online behavioural advertising, and continued its dialog with the largest providers of online search engines (Google, Yahoo, Microsoft) and with providers of online social networks regarding the protection of young users (Facebook and others). Within the framework of the Future of Privacy Sub-Group, the Information Commissioner, together with German colleagues, prepared a standpoint regarding the existing regime and changes to the legislative order in the field of sensitive personal data.

In 2010, the Head of the Information Commissioner continued to hold the position of Vice-Chairman of the Europol Joint Supervisory Body. At the end of January, the Information Commissioner hosted a two-day meeting of members of the Europol, Eurojust, Schengen and Customs Joint Supervisory Authorities in Ljubljana, where discussions were held on the future of the Joint Supervisory Authorities in light of the adoption of the Lisbon Treaty.

With the entry of the Republic of Slovenia into the Schengen area, the Information Commissioner also became competent to supervise implementation of Article 128 of the Schengen Convention and thus it represents the independent authority responsible for supervision of the transfer of personal data for the purposes of the Convention. In 2010 the Information Commissioner did not receive any complaints regarding the exercise of this right at the first instance.

In the framework of its national competence to supervise the protection of personal data, the Information Commissioner carried out an inspection of the Metlika border police station with regard to the Vinica international border crossing and reviewed the lawfulness of personal data processing in the Schengen Information System (SIS).

The Information Commissioner also regularly participated in the meetings of the Working Party on Peace and Justice (WPPJ), which in 2010 were focused primarily on the exchange of personal data between the European Union and the United States of America, the processing of DNA data by prosecuting authorities, monitoring the implementation of the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, as well as other general issues relating to personal data protection in the framework of the Lisbon Treaty.

The Information Commissioner also actively participated in the International Working Group on Data Protection in Telecommunications (IWGDPT), in the frame of which representatives of information commissioners and personal data and privacy protection authorities from all over the world meet. The working group adopted the following documents at sessions in Granada and Berlin: Working Paper on Mobile Processing of Personal Data and Security, Working Paper on the Use of Deep Packet Inspection for Marketing Purposes, the Granada Charter of Privacy in a Digital World and the Working Paper on Privacy Risks in the Re-Use of Email Accounts and Similar Information Society Services.

Once again in 2010, 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). At its plenary session in June, the T-PD Committee finished preparations for its important Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling, which the Committee of Ministers adopted in

November 2010. Every year the T-PD Committee also discusses the reports of the supervisory authorities for the protection of person data of the member states of the Council of Europe, and in the future it will focus primarily on preparations for amending and modernising Convention 108.

In 2010, the Information Commissioner also participated in the inspection group which carried out supervision of personal data protection at the European Union's Judicial Cooperation Unit (Eurojust) at its headquarters in the Hague.

In 2010, the Information Commissioner hosted representatives of the Polish, Hungarian, and Kosovar authorities responsible for ensuring personal data protection and access to public information. Information Commissioner staff members prepared numerous presentations of their work for the representatives of these authorities.

Information Commissioner inspectors had a one-week expert training programme at the Hungarian authority responsible for ensuring personal data protection and access to public information.

From April to July 2010, the Information Commissioner hosted a grant recipient from the European Fund for the Balkans.

In 2010, the Information Commissioner prepared responses to 38 questions of foreign data protection authorities, international organisations, and foreign non-governmental organisations.

In a consortium with the Ludwig Boltzmann Institute for Human Rights from Austria, the Information Commissioner was selected for the implementation of the twinning project IPA 2009, No. MN/09/IB/JH/03 – Implementation of Personal Data Protection Strategy in Montenegro. The project focused on the establishment of a national data protection authority in Montenegro, staff education, and the building and implementation of the legal framework for personal data protection in the country and closer cooperation between Montenegro and the EU. Project activities began in November 2010 and will continue until 2012.

Last year the Information Commissioner began to participate in the European project LAPSI (Legal Aspects of Public Sector Information), which is financed by the European Union on the basis of contract no. 250580 of the European Commission, with the coordinator of the project Politecnico di Torino. The project is focused on detecting and eliminating legal barriers to accessing and re-using public information which occur in the fields of law, informatics, intellectual property, privacy, and competition, administrative, and environmental law, and on formulating strategies for overcoming such barriers.

Last year the Information Commissioner completed the EU-financed project European Privacy Open Space, which had been running since 2008, under the leadership of Unabhängiges Landeszentrum für Datenschutz from Germany.

The Annual Report was prepared by:

Editor:

Nataša Pirc Musar, Head of the Information Commissioner

Text:

Dr. Monika Benkovič Krašovec, State Supervisor for the Protection of Personal Data
Jože Bogataj, Head of State Supervisors for the Protection of Personal Data
Eva Kalan, Advisor
Nina Komočar, Researcher
Tina Kraigher, Researcher
Kristina Kotnik Šumah, Deputy Information Commissioner
Rosana Lemut-Strle, Deputy Information Commissioner
Andrej Tomšič, Deputy Information Commissioner

Translation:

Petra Zaranšek and **Dean J. DeVos**

Address:

Informacijski pooblaščenec RS
Vošnjakova 1
1000 Ljubljana
Slovenija

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

Ljubljana, June 2011

ISSN 1854-9500