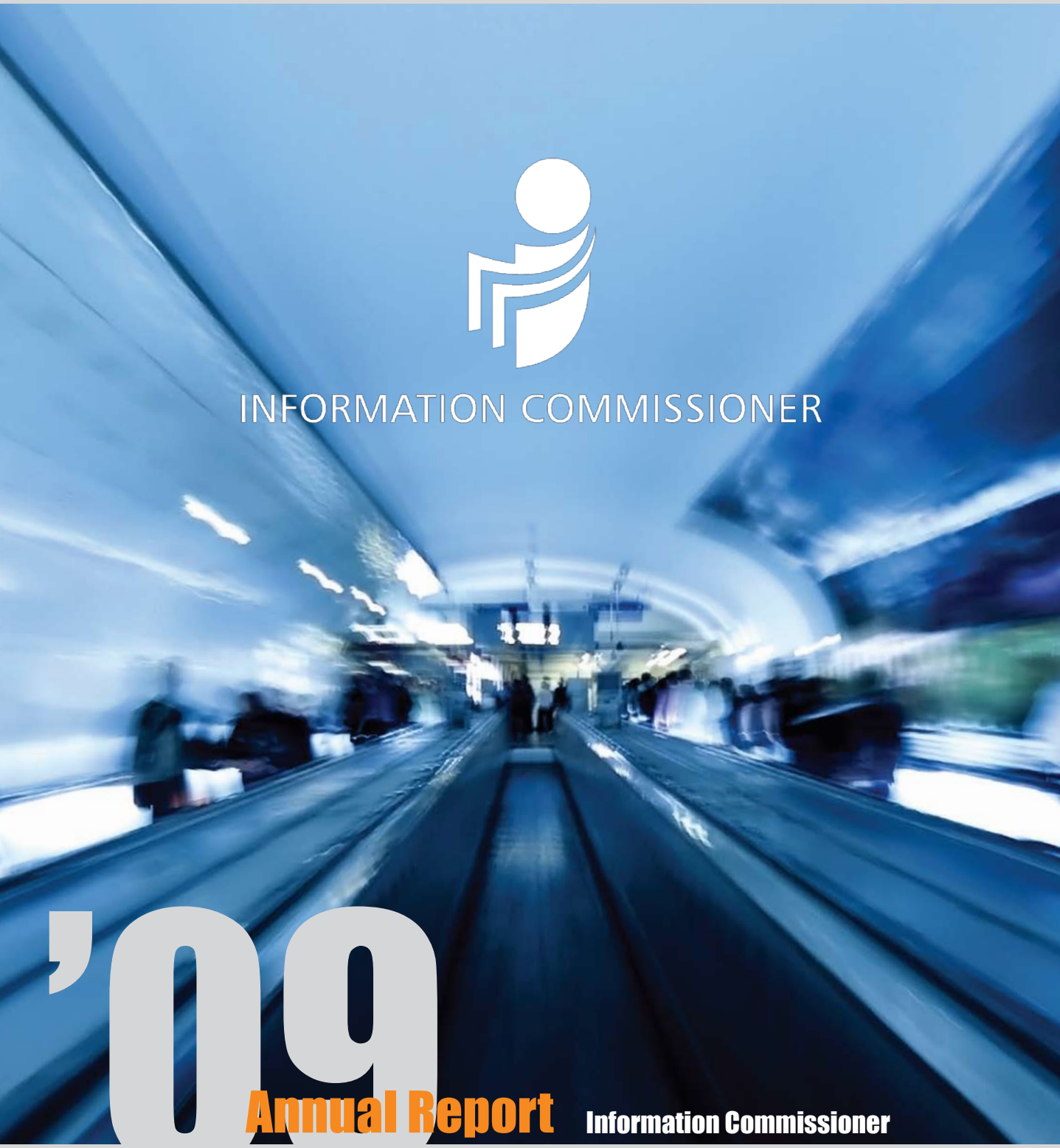


INFORMATION COMMISSIONER

'09 Annual Report

Information Commissioner

2009

'09 Annual Report

Information Commissioner

2009

0 INTRODUCTION

In 2009, the work of the Information Commissioner of the Republic of Slovenia was marked by issues pertaining to a significant increase in the exercise of the right of individuals to free access to information as well as the right to the protection of personal data. The results of public opinion polls have revealed that the general public has maintained its confidence in the Information Commissioner, which is consistently placed at the very top of surveys into the most trustworthy institutions in Slovenia. On 21 May 2009, following a proposal by the President of the Republic of Slovenia, Dr. Danilo Türk, the National Assembly of the Republic of Slovenia renewed my mandate for a further five years; I regard this not only as a personal vindication, but as a further expression of trust in the work of the Information Commissioner.

In accordance with Article 14 of the Information Commissioner Act, the Information Commissioner has prepared a Report as to its operations during 2009; accordingly, in May 2010, this Report has been submitted to the National Assembly of the Republic of Slovenia. I am pleased to have established for a fourth successive year that the level of respect and awareness as to the right of free access to information as well as the right to the protection of personal data continues to increase, and that the Information Commissioner has successfully dealt with numerous new challenges.

The number of formal complaints lodged by journalists under the Mass Media Act and the Access to Public Information Act increased significantly during 2009. The complaints that the Information Commissioner has dealt with are becoming ever more complex and ever more voluminous as regards the number of documents which are the subject of deliberation. During 2009, the Information Commissioner handed down significantly more decisions pertaining to access to public information than it did in 2008 (129 were delivered in 2008, rising to 161 in 2009).

In particular, the number of complaints consequent to implied decisions has risen significantly (259 in 2008, and 302 in 2009), as has requests for various explanations (102 such requests were received in 2008, rising to 328 in 2009). The underlying reason for this may be that the activities of the Ministry of Public Administration are insufficient in this field. It is a fact that the Access to Public Information Act imposes numerous obligations upon public authorities, which they are unable to carry out without the necessary knowledge, financial and personnel resources, as well as the provision of professional assistance by the competent ministry.

The Information Commissioner has established precedent in this field during the six years of its operation, and this has been further advanced and consolidated by the decisions of the Administrative Court of the Republic of Slovenia. Said Court adopted some important decisions during 2009, amongst others that complaints against the levy of fees for access to public information is permitted, and that the appellate body in such instances is the Information Commissioner. Herein we would yet again like to warn that the non-critical charging of

fees for access to public information may seriously jeopardize the entire system of access to public information. The Information Commissioner thus advises against the use of any tariff which enables the arbitrary and uncontrolled levy of fees for the transmission of public information.

Based on the executed appeal procedures, the Information Commissioner assesses that the liable authorities as well as the applicants are better informed as regards access to public information, and that liable persons now publish significantly more information over the Internet, even prior to any actual receipt of requests by applicants.

In inspection cases and requests for opinions in relation to the field of personal data protection, the Information Commissioner encounters evermore complex and demanding challenges as regards upholding information privacy. Offences and irregularities, established in the field of personal data protection during 2009, are very much the same as those documented in previous years. In 2009, the Information Commissioner imposed its highest fine yet (102,000 Euros) in relation to two insurance companies. The fine was levied as a consequence of the illegal processing of personal data pertaining to 2,382 former insured persons, whose personal details were transferred from one insurance company to the other without any appropriate legal basis for such; said data was then used for direct marketing.

During 2009, the Information Commissioner continued with its ex officio inspection procedures in various parts of Slovenia, and more than one hundred such inspections were carried out in the course of the year. Among the targets of these inspections were the controllers of large personal data collections, encompassing such compilations as employee personal data, customer relations management systems and the issuers of loyalty cards, the operators of electronic communications systems, tourist facility providers and libraries.

Last year, the Information Commissioner dedicated a deal of attention to the question of employee expectations of privacy in the workplace, especially in relation to the use of corporate email, telephones and computers that are - to some extent - also used by the employees for private purposes. This area still reveals the pressing problem of a lack of legal regulation, in relation to which the Information Commissioner has issued several warnings. Last year, in order to resolve such dilemmas, the Information Commissioner drafted a Communication Privacy in the Workplace white paper, which was forwarded to the Ministry of Labour, Family and Social Affairs; unfortunately, however, no further action has been announced in this field.

In the health service, the Information Commissioner still encounters numerous cases which reveal an inappropriate approach to personal data protection. The handling of a person's sensitive medical data is a most crucial issue, and a profound change in attitudes towards its protection is necessary, as is the introduction of an integrated and systematic approach to the protection of information, which should be based on internationally established standards, such as, for example, ISO/IEC 27001. Further to Article 14 of the Personal Data Protection Act, some changes in legislation should also be considered in relation to protection, and such would increase the level of requirements for the controllers of sensitive personal data filing systems.

The Information Commissioner faced numerous dilemmas in the field of electronic communications, particularly in relation to the mandatory storage of electronic communications data. The Information Commissioner thus carried out ex officio inspections which revealed that the protection of stored data is - in the majority of cases - appropriate; major deficiencies were, however, primarily discovered in relation to smaller telecommunications operators.

As in previous years, the Information Commissioner has enjoyed good co-operation with all state bodies, and thus the need to resort to negative exposure has not arisen. Expert arguments, expressed in remarks to legislation and statutory procedures, contribute to improved regulatory processes as well as the enhanced institution of both the right of access to public information and protection of personal data. Special attention has been dedicated to the assessment of the impact of legislation on privacy, and we cooperated in a variety of projects pertaining to the merging of personal data collections, such as the establishment of the National Investigation Bureau and a series of projects in the field of eUprava (e-Administration) - including eZdravje (eHealthcare), eSociala (eSocial Services), eVEM (for companies), eSJU (administration) and eArhiviranje (archiving). The Information Commissioner was also

involved in public administration information security policy, as well as SRITES - the strategy for the development of information technology, electronic service provision and the merging of records.

In its supervision of the implementation of the Personal Data Protection Act, the Information Commissioner established some deficiencies and indeterminate issues, which reveal that the Act should be supplemented and amended. In order to eliminate the deficiencies and imprecise issues, the Information Commissioner prepared a proposal for amendments and supplements to this legislation, and this has been passed on to the Ministry of Justice for further deliberation.

During 2009, the Information Commissioner dedicated considerable attention to preventive activities. In relation to those specific areas proving to be most vexatious, it also produced several publications (including How to Use Facebook and Survive, Privacy in the Workplace and Personal Data Protection and the Media) as well as numerous guidelines (five of which were also issued in the English language).

Throughout the year the Information Commissioner also endeavoured to inform everyone - the public at large, as well as legal entities and other organisations - as to the nature of its work. It ensured that its activities were made known to all and sundry. Information was provided directly via the website http://www.ip-rs.si/ as well as through regular and ongoing contacts with the media, as well as - of course - through direct communication with those responsible and liable. The Information Commissioner's expert staff also participated in numerous conferences, congresses and panel discussions over the course of the year. During 2009, the Information Commissioner again marked the Personal Data Protection Day as well as the Right to Know Day.

In order to improve information provision to both expert as well as lay publics, the Information Commissioner continues to endeavour to maintain its user-friendly website. All legal opinions pertaining to personal data protection and decisions pertaining to access to public information are published on it. At the end of 2009, the Information Commissioner created its own profile on the social networking site Facebook. It was probably the first such institution to do so, and thus introduced a new channel of communication for the wider public to be able to communicate with the Information Commissioner and to be informed about it's activities..

Through its co-operation with working groups and monitoring authorities, the Information Commissioner continues to actively contribute to the development of rights in relation to access to information and the protection of personal data at the European and international levels. In June 2009 Slovenia became one of the first countries to sign the Council of Europe Convention on Access to Official Documents. Besides which, last year I personally became the Vice-President of the Joint Supervisory Body of Europol, the body that oversees this important European institution which processes a large amount of personal data in the course of its work.

Despite the increased scope of its operations, numerous new responsibilities and enhanced international engagement, the number of Information Commissioner personnel was not increased last year due to the implementation of cost-saving measures. The office of the Information Commissioner had 32 employees as of 31 December 2009.

It is my sincere hope that in 2010 and 2011 we can achieve a greater degree of responsivity from the competent ministries in relation to legislative proposals that pertain to access to public information and the protection of personal data. I also wish that those who have the opportunity to make decisions, become aware that removing the possibility of the Information Commissioner's access to the Constitutional Court - this highest protector of fundamental human rights in Slovenia - for those areas for which it is competent, is neither reasonable nor substantiated.

Nataša Pirc Musar, LL.M.
Information Commissioner of the Republic of Slovenia

INTRODUCTION

1 INFORMATION COMMISSIONER

1.1. Establishment of the Information Commissioner

On 30 November 2005 the National Assembly of the Republic of Slovenia passed the Information Commissioner Act[1], on the basis of which an independent state body was founded on 31 December 2005. By way of the aforementioned Act the bodies of the Commissioner for Access to Public Information, in the past an independent body, and the Inspectorate for Personal Data Protection, a constituent body within the Ministry of Justice, were amalgamated. With the implementation of the Information Commissioner Act, the Commissioner for Access to Public Information continued its work as Information Commissioner, assuming the supervision of the inspectors and other employees of the Inspectorate for Personal Data Protection and its pertaining resources. At the same time, all outstanding operations, archives and records of the Inspectorate for Personal Data Protection came under its supervision. Thus the jurisdiction of the office that had previously been responsible for the unimpeded access to public information evolved and expanded to encompass the protection of personal data. In this manner, the Information Commissioner became a national supervisory authority for personal data protection and commenced operations on 1 January 2006.

This regulation, which is comparable with that in other EU states, enabled a level of uniformity between the state bodies. At the same time it also promotes awareness about the right to privacy and the right to information – and their mutual interdependence comes to the fore. Appointed by the National Assembly of the Republic of Slovenia, on the basis of a proposal by the President of the Republic of Slovenia, the Information Commissioner is headed by Ms. Nataša Pirc Musar, who on 21 May 2009, following a proposal by the President of the Republic of Slovenia was renewed her mandate for a further five years, starting 16 July 2009.

1.2. Jurisdiction of the Information Commissioner

Under Article 2 of the Information Commissioner Act, the Information Commissioner is competent to:

- decide as to complaints against decisions by way of which an authority has rejected a request or in any other way withheld the right of access to, or re-use of, public information; and, with regard to procedures at a second instance, also in the supervision of the enforcement of the law that regulates access to public information as well as in oversight of the regulations issued on the basis of the aforementioned law;
- inspect the enforcement of law and other statute that regulate the protection and processing of personal data, the transfer of personal data from the Republic of Slovenia, as well as the performance of other duties defined by these regulations;
- decide as to complaints made by individuals when the data controller denies the request of an individual regarding their right of familiarization with the requested data, extracts, lists, access, certificates, information, clarifications, true copies or copies under the provisions of the law that regulates the protection of personal data;
- lodge an application at the Constitutional Court of the Republic of Slovenia for a constitutional review of law, other regulations and general acts brought into force for the purpose of implementing public powers with regard to a procedure being conducted in relation to access to public information or the protection of personal data.

The Information Commissioner has jurisdiction of an appellate body under the Public Media Act[2]. According to the Public Media Act the refusal of a liable authority to answer a

[1] Official Gazette of RS, No. 113/2005 – 51/2007-Constitutional Court Act-A; ZinfP.
[2] Official Gazette of the Republic of Slovenia, No. 110/2006, official consolidated text 1 with amendments; ZMed.

question posed by a representative of the media shall be considered as a rejection decision. The silence of an authority in such an instance is an offence, as well as grounds for a complaint. A complaint against a rejection is permitted if the negative reply to the question pertains to a document, case, file, register, record or other such archive. The Information Commissioner makes a decision as to a complaint against a rejection decision under the provisions of the Access to Public Information Act[3].

The Information Commissioner also has the function of a violations body, whose jurisdiction is the supervision of the implementation of the Information Commissioner Act, the Access to Public Information Act with regards to the appeal procedure, the provision of article 45 of the Public Media Act and the Personal Data Protection Act[4].

Pursuant to the second paragraph of Article 112 of the Electronic Communications Act[5], the Information Commissioner supervises the safekeeping of traffic and locational data obtained or processed in relation to the provision of public telecommunications networks and services. In accordance with the first paragraph of Article 147 of the ZEKom, the Information Commissioner also acts as a body responsible for the address of misdemeanours in the provision of public telecommunications networks and services.

Upon Slovenia's accession to the Schengen zone, the Information Commissioner also took charge of the supervision of the implementation of Article 128 of the Schengen Agreement. The Information Commissioner henceforth represents an independent supervisory authority for the regulation of personal data transfer in accordance with the Schengen Agreement.

Pursuant to Article 114 of the Convention implementing the Schengen Agreement, each contracting member state shall designate a supervisory authority which shall, in accordance with national law, be responsible for the independent supervision of the data file of the national section of the Schengen Information System, as well as for ensuring that the processing and use of data entered into the said System does not violate the rights of the data subject. A joint supervisory authority shall be responsible for supervising the technical support function of the Schengen Information System as regards personal data protection, whereas the national supervisory authority of each contracting state – in Slovenia: the Information Commissioner – shall be responsible for the supervision of the national data collection.

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

The competences of the Information Commissioner arising from the Patients Rights Act are as follows:

- Ruling as to complaints by patients and other eligible persons in cases of alleged infringement of the provision regulating the manner of familiarization with medical documentation; whereas the provider of medical services is, in this procedure, regarded as the first instance authority (tenth paragraph of Article 41 of the ZPacP);
- Ruling as to complaints by persons, defined by the Act, against partial or total rejection of any request for familiarization with medical documentation following the death of a patient (fifth paragraph of Article 45 of the ZPacP);
- Ruling as to complaints by eligible persons against partial or total rejection of any request for familiarization pertaining to the obligation of protection of information as to the medical condition of a patient, providing that the requested information arises from medical documentation (seventh paragraph of Article 45 of the ZPacP).

[3] Official Gazette of the Republic of Slovenia, No. 51/2006 and 117/2006-ZDavP-2; ZDIJZ.
[4] Official Gazette of the Republic of Slovenia, No. 94/2007 - official consolidated text; ZVOP-1.
[5] Official Gazette of RS, No. 13/2007 official consolidated text 1 with amendments; ZEKom.
[6] Official Gazette of RS, No. 15/2008; ZPacP.
[7] Official Gazette of RS, No. 62/2009 – official consolidated text 3; ZPLD.
[8] Official Gazette of RS, No. 71/2008 – official consolidated text 2; ZOIzk.

The competences of the Information Commissioner in relation to the Identity Cards Act:

- Supervision under Article 3.a, which regulates the instances and the manner in which the data controller is allowed to copy identity cards, as well as the manner in which copies may be kept (safekeeping);
- In the event of any infringement of the provision under Article 3.a, the Information Commissioner shall, as the competent authority, rule in accordance with Article 19.a.

The competences of the Information Commissioner pertaining to the Travel Documents Act:

- Supervision in relation to Article 4.a, which regulates the instances and the manner in which the data controller is allowed to copy travel documents, as well as the manner in which copies may be kept (safekeeping);
- In the event of any infringement of the provision under Article 4.a, the Information Commissioner shall, as the competent authority, rule in accordance with Article 34.a.

In 2009, the Information Commissioner also granted competencies under the Banking Act.[9]

- gives its assent to the administrators of the SISBON system prior to the application of system's rules from Item 1 of the paragraph 13 of the Article 309a, which provides that he administrator must accept the rules of the system, where he sets forth technical conditions for the access to the system and other measures for the protection of personal daza (indent 14 of Article 390.a);
- exercises supervision over Article 309.1, which sets forth the cololection and processing as well as the system on the exhange pf informationon the credit rating of the customers (SISBON syste,) and conducts offence proceedings due to the infringement of thze provisio0ns of Article 309 a(10-15 indent of Article 397), all in compliance with Article 397.

1.3. Organization of the Information Commissioner

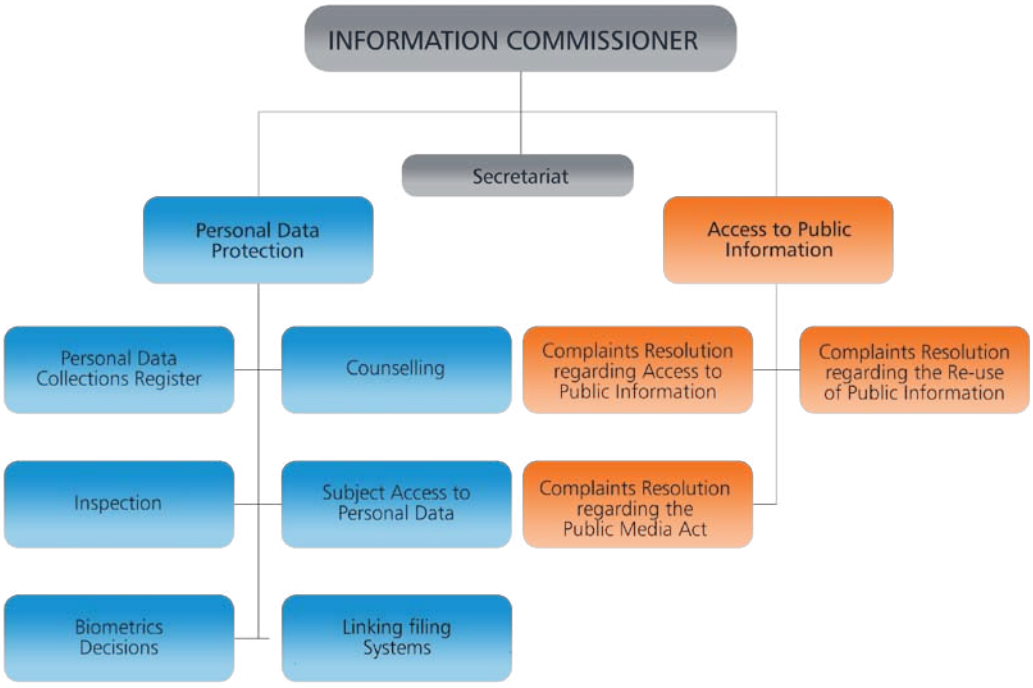
The internal organization, staff deployment and operations of the Information Commissioner in the context of its tasks, functions and mandates are prescribed by the Regulations on cadre, posts and professional titles at the Information Commissioner. The cadre and deployment of personnel is adjusted to the ongoing tasks and work processes, and is designed to ensure the maximum utilization of available human resources.

The Information Commissioner performs its operations through the following internal organisational units:

- The Secretariat,
- Public Information Department,
- Personal Data Protection Department,
- Admin and Technical Department.

[9] Official Gazette of RS, No.131/2006, with amendments ; ZBan.

Diagram 1: Organization



At the end of 2009, the Information Commissioner had 32 personnel, two of them employed on temporary basis. The number of employees has not changed in comparison with 2008. All those working as civil servants within the organisation have university degrees.

1.4. Finances

The work of the Information Commissioner is financed from the state budget; funding is apportioned by the National Assembly of the Republic of Slovenia (Article 5 of the Information Commissioner Act). In fiscal year 2009, the funding initially allocated to Information Commissioner amounted 1,319,809.00 euros. The Ministry of Public Administration provided the Information Commissioner with 21,059.00 euros for wage disparity elimination. Within the framework of participation at the European project European Privacy Open Space Information Commissioner received 14,400.00 euros recorded under the Item 9378 (»European funds for cooperating in the project«) for the purposes of participating in the project. The Information Commissioner reallocated 22,298.96 euros from the Item 1271 (»material costs and expenses«) to the Item 1267 (»wages and salaries«) and 6,474.05 euros onto the Item 1273 (»investments«). In 2009, earmarked funds brought forward from 2008 amounted to 3,725.11 euros on the Item 7459 (»tangible assets – acquisition assets«) and the Item 7460 (»tangible assets – indemnification assets«) (adopted budget did not consider the aforementioned items).

During fiscal 2009, the Information Commissioner had spent 1,325,926.19 Euros, namely:

- 998,804.37 Euros for salaries and other employee expenses;
- 300,647.77 Euros in material costs;
- 26,474.05 Euros in investments and capital expenditure.

Accordingly, 99.27 % of the available budget for 2009 had been used during the course of the year.

2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

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

The legislator has ensured the right of access to public information through 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 of access to public information is a fundamental human right, and has, as such, been included in the Constitution, it was not until twelve years after the Constitution had been adopted, that this right was enshrined through statute, namely, through the passing of the 2003 Access to Public Information Act[11]. Up until then, individual provisions with regard to public information had been part of certain disparate pieces of legislation; today, however, the Access to Public Information Act now comprehensively regulates these issues. This Act was endorsed by the National Assembly of the Republic of Slovenia in February 2003, and it entered into force on 22nd March 2003.

A step forward was made in 2005 through the passing of an amendment to the Access to Public Information Act, the amendment namely lessened the possibility for undue obstruction of access to information and introduced numerous innovations, such as the re-use of public information, and the jurisdiction of administrative inspection in the enforcement of the provisions of said Act. However, it was the public interest test that was the most important novelty. The amendment also emphasized the openness of data concerning the spending of public funds as well as data concerning the employment relationship and the carrying out of public functions. Thereby Slovenia joined those democratic countries in which, when it comes to public interest, exceptions are treated with reservation.

2.2. Review of Activities in the Field of Access to Public Information in 2009

182 complaints against the decisions of authorities that rejected requests for access to the use or to the re-use of public information were lodged during 2009. The Information Commissioner issued 161 decisions, in nine cases the complaints were rejected with a decision, while the Information Commissioner surrended four claims to be decided upon by the competent authority, and one individual withdraw his complaint. The number of decisions in the field of access to public information has significantly increased compared to 2008, when 129 decisions were issued.

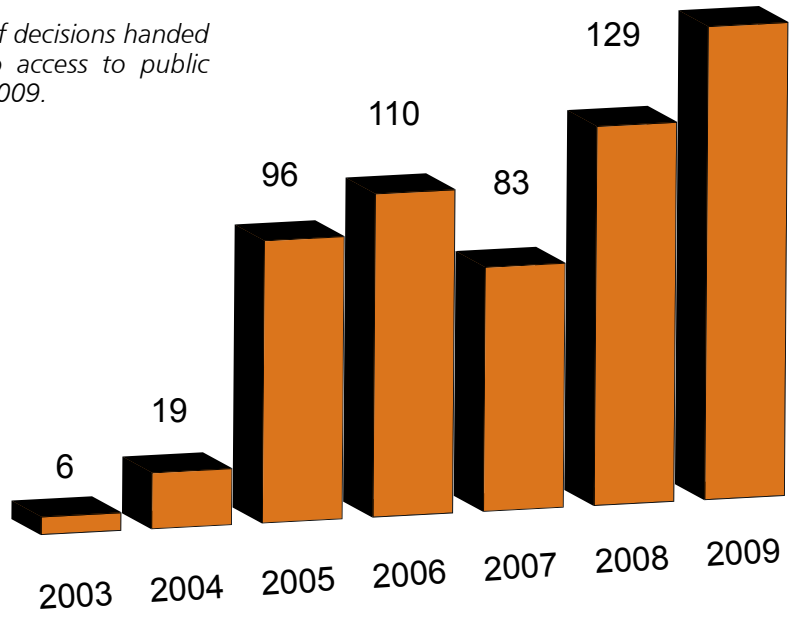
As regards the decisions the Information Commissioner:

- rejected the complaints in 60 cases,
- resolved the matter in favour of the applicants in 57 cases,
- partially approved access in 29 cases and
- returned the matter to the first instance authority in 13 cases,
- in two cases the Information Commissioner rejected the complaint as inadmissible.

[10] Official Gazette of the Republic of Slovenia, Nos. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004 and 68/2006; the Constitution of the Republic of Slovenia.

[11] Official Gazette of the Republic of Slovenia, No. 24/2003; ZDIJZ.

Picture 2: Number of decisions handed down in relation to access to public information, 2003-2009.



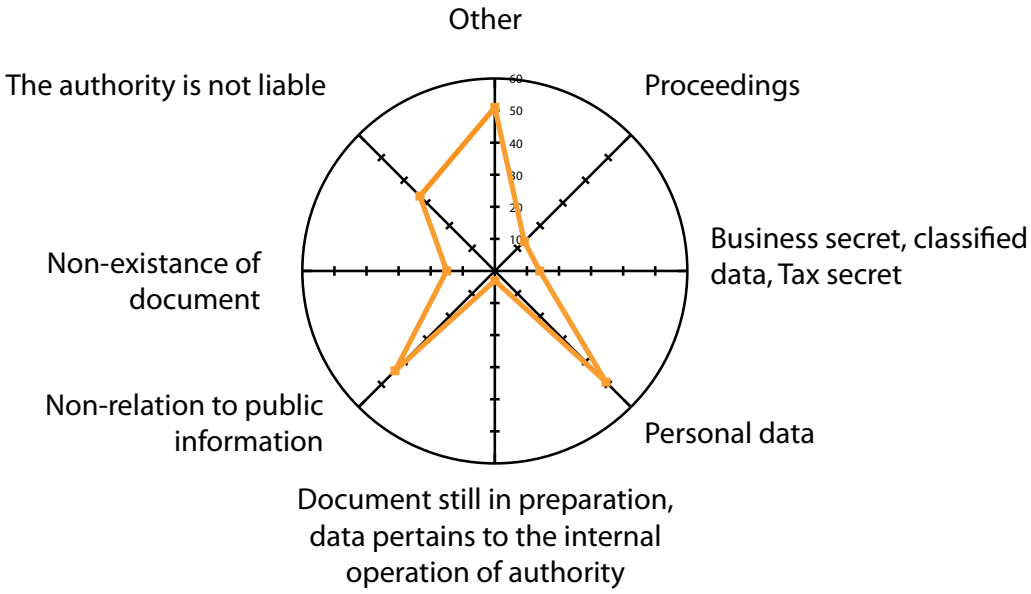
The Information Commissioner's decisions concerned and/or involved review as to:

- whether the requested documents included personal data, the disclosure of which would contravene the provisions of the Personal Data Protection Act (51);
- whether the liable person or authority holds the document or the public information which has been requested by the applicant (49);
- whether the applicant requested information and/or data considered a business secret, according to the act regulating companies (28);
- whether the requested document fulfilled the conditions for the existence of public information in accordance with the 1st paragraph of Article 4 of the Access to Public Information Act (14);
- whether the requested information pertains to data in documents drafted in relation to the internal operations or activities of the authority, the disclosure of which could cause disturbance to the operations and/or activities of the authority (9);
- whether the requested information is protected in accordance with the act regulating copyright; in any such instance the applicant shall be granted access to the data for the purposes of familiarization (9);
- issuing a decision in an instance the applicant was a journalist (8);
- issuing a decision in an instance the applicant requested a document pertaining to a public procurement procedure (8);
- whether the requested information was data acquired or put together on the basis of a criminal prosecution or violations procedure, the disclosure of which would be deleterious to the implementation of the procedure (6);
- whether this is an instance of violating the rules of procedure (6);
- whether the requested information contained data that was acquired or put together on the basis of a civil, non-contentious civil proceeding or any other court proceeding, the disclosure of which could bring upon the implementation of such proceeding detrimental effects (5);
- the serving of public interest; namely whether public interest in disclosure is stronger than the public interest, or the interest of other persons, in the constraint of access to the requested information (4);
- whether the requested information is data pertaining to documents still under

preparation and thus subject to internal consultation, further to which premature disclosure could result in misinterpretation as to their content (4);
- whether the requested information contained data that was classified (as an official secret) on the basis of the law regulating classified data (4);
- whether the requested information contained data that was acquired or put together on the basis of an administrative procedure, the disclosure of which could bring upon the implementation of such procedure detrimental effects (4);
- whether the authority, to which the request for public information was addressed, is liable to provide information in accordance with 1st paragraph of Article 1 of the Access to Public Information Act (3);
- whether this is an instance of the re-use of public information (3);
- whether this is an instance of the abuse of a right granted pursuant to the Access to Public Information Act (3);
- whether the requested information encompasses data, the disclosure of which would be an infringement of confidentiality re a tax procedure or the institution of tax secrecy, in accordance with the act regulating tax procedures (1);
- whether this is an instance of a right granted pursuant to the Access to Public Information Act (1);
- whether the Access to Public Information Act having a retroactive effect (1);
- whether this is an instance of the archive material (1).

In 2009, the Information Commissioner issued five decisions in cases in which complaints had been filed at the administrative court which ruled that the Information Commissioner must reconsider its decisions in regard to those cases.

Picture 3: Decisions taken in relation to the Access to Public Information Act with regard to various exemptions (N.B. a single decision may refer to several exemptions).



Complaints lodged by applicants as the result of a rejection of access to public information concerned the following groups of liable authorities:
- Ministries and their constituent bodies (46),
- Public funds, institutes, agencies and other entities subject to public law (41),
- Administrative units and municipalities (40),
- Courts, the Office of the State Prosecutor General, and the Attorney General's Office (21),
- Educational institutions (8),
- Health authorities (4).

One complaint in relation to private sector entities proved to be ineligible according to the Access to Public Information Act.

109 applications were lodged by private individuals, and in 11 occasions NGOs, various associations, societies and trade unions. In 27 instances private sector legal entities, lodged complaints as to the lack of provision of requested information; the Information Commissioner also received 12 complaints lodged by journalists, one complaint by a municipality and one by a public sector legal entity (university).

In 2009, 26 lawsuits were filed at the Administrative Court against decisions made by the Information Commissioner, a figure which represents 16% of the adopted decisions. The relatively small number of lawsuits points to the establishment of a higher degree of transparency and openness of public sector authorities regarding their activities, as well as the acceptance of the Information Commissioner's decisions by the various bodies and applicants. As of the end of 2009, the Administrative Court had rendered 14 judgements in lawsuits against the decisions made by the Information Commissioner. In two instances the contested decision was annulled and the matter returned to the Information Commissioner for reconsideration; in 12 cases the Administrative Court rejected the complaints. In 2009 the Supreme Court decided upon three cases in which the plaintiff did not agree with the Administrative Court's judgement. In all these cases the Court rejected the appeals and upheld the contested judgements.

In 2009, the Information Commissioner received 302 complaints consequent to implied decisions, namely, instances in which an authority had failed to reply to the applicant's request. In such instances the Information Commissioner asked the authority to decide as to the applicant's request as soon as possible, subsequent to which in as many as 228 cases the liable body granted an applicant access to the requested information, in 29 instances the Information Commissioner rejected the complaint with a decision, seven individual withdrew their complaints, while in the remaining instances the authorities rejected to replay to the applicants; consequently these applicants re-lodged their complaint with the Information Commissioner who then ruled with a decision.

In answering complaints filled by individuals, access without the present of parties and public was required at times, i.e. in camera access, by way of which the Information Commissioner establishes the actual situation of the document, held by the authority in question. In 2009, 61 such accesses in camera were performed.

328 requests for help and various questions posed by individuals (207 of which were sent via an electronic mail) were addressed to the Information Commissioner during the course of 2009, these related to access to public information, especially regarding the question whether a certain document should be in the public domain. Within the scope of its authority, the Information Commissioner replied to all of these requests, and in most cases referred the correspondent to the competent authority.

In 2009, no offence proceeding was instigated in the field of access to information of public character.

2.3. Some Significant Cases and Precedants in Individual Areas

By way of its Decision No. 090-18/2009/39, of 18 November 2009, the Information Commissioner deliberated 11 appeals in relation to the Municipality of Žužemberk, which had denied an applicant's request on the basis of the misuse of the right of access to public information. After having studied the entire case, the Information Commissioner established that no legitimate reasons had been provided by the Municipality, on the basis of which the actions of the applicant could be defined as a misuse of the right of access.

In order for a misuse of a right to exist, the pre-condition of a conflict of two non-exclusive rights has to be established; such a conflict of rights is thus a necessary prerequisite for there to be the possibility of the misuse of a right. The Municipality maintained that in this instance there was a collision between the applicant's statutory right and the rights and duties of the Municipal authority to execute its local administrative function and budget resources in compliance with the Local Government Act[12], the Financing of Municipalities Act[13], its internal statute as well as other public finance regulations. However, no detailed reasoning or explanation of this was provided by the Municipality, hence and such collision was mere conjecture and thus hypothetical.

The Municipality also stated that the applicant was acting with the purpose of impairing the work of the Municipality and its employees, and that the volume of the requests of the applicant would require the employment of an additional employee, which would increase costs, and was not feasible in the context of budgetary constraints; further to which, the volume of the applicant's requests seriously jeopardized the execution of other tasks, which needed to be carried out by Muncipality, and thus it could not afford to dedicate an employee solely to working on the applicant's requests and applications.

After studying the Municipality's rights, the Information Commissioner concluded that it is not possible to rationally foresee which actual right of the Municipality would collide with the right of the applicant in his request for public information, and thus the Information Commissioner concluded that in this instance the basic pre-condition - which represents the basis for any misuse of a right - had not been fulfilled. Dissemination of public information is one of the statutory tasks of the Municipality, hence it is legally obliged to provide the necessary means and personnel for the fulfilment of such requests. The Information Commissioner likewise affirmed that the Municipality should provide the applicant with the documents requested.

By way of its Decision No. 090-74/2009 of 25th November 2009, the Information Commissioner ruled on an applicant's appeal in relation to the decision of the Oskar Vitovlje pet shelter (an organisation accommodating, caring for, grooming and training pets and lost animals – henceforth: OV), by means of which OV declined access to the contracts which it had concluded with municipal authorities in relation to dealing with abandoned animals. The Information Commissioner established that OV, as a public service contractor providing animal shelter services, belongs to those bodies which are liable under paragraph 1 of Article 1 of the Access to Public Information Act.

The extent of OV's work and contractual obligations within the scope of its executing a public service contract was disputable. Based on paragraph 2 of Article 27, as well as paragraph 2 of Article 31, of the Animal Protection Act[14], Information Commissioner established that the OV shelter, to which the municipality had transferred the execution of some or a number of its public service provision obligations by means of a contract, had thereby become a public service contractor, namely the executor of public services under administrative law. The contract on the transfer of the public service is a key document, on the basis of which the

[12] Official Gazette of RS No. 72/1993, with amendments; ZLS.
[13] Official Gazette of RS No. 123/2006, with amendments; ZFO.
[14] Official Gatette of RS No. 43/2007; *ZZŽiv*.

public service provision is thence implemented; hence such a contract undoubtedly pertains to the domain of the work of contractor within its provision of the said public service/s.

The Information Commissioner has established that OV's argument - namely that the data under such contracts should be regarded as a business secret - would not stand up to legal challenge. The data - which is actually stated in the requested documents - sets forth the terms and conditions as well as the method of implementing the public service, none of which is related to the institution of a business secret or impacts the competitive position of the subject. Accordingly, the Information Commissioner concludes that the contracts under consideration wholly represent information in relation to public service provision, which should be freely accessible.

By way of its Decision No. 090-78/2009 of 4 August 2009, the Information Commissioner ruled on an appeal in relation to a decision issued by Pošta Slovenije d.o.o. (Slovenia's national postal services provider - henceforth: PS), which rejected a request by an applicant in relation to a public tender process. The tender for the provision of mailbags was carried out in 2008, and the applicant requested photocopies of the entire bidding documentation submitted by the bidder Erhart d.o.o., the tender and other documents issued by the principal (PS) in relation with the tender procedure, as well as well as the results of the analysis of the mailbags and their materials (submitted by the bidders Jerič Nevenka, s.p. and Erhart d.o.o.) which the principal had ordered from the Maribor University Faculty of Technology, or some other institution, and pertained to the appropriateness of the materials in relation to said tender.

In this appeal procedure, the Information Commissioner deliberated whether PS justifiably supported its rejection of the request on the basis of the existence of a business secret. The Information Commissioner established that certain requested data does represent the business secret of a secondary party, under subjective criteria in accordance with the Companies Act[15]. The Information Commissioner also assessed whether the condition was met under which certain data is - according to law - is public; namely if said data pertains to the use of public finance.

PS did not select any bidder in the said procedure, so there was no instance of any use of public finance and hence, from the aspect of public supervision over their work, it is completely irrelevant whether the un-chosen bidders in an unaccomplished tender have met all the tender specifications or not. The Information Commissioner also assessed that the public interest for the disclosure of the requested information is not stronger than the interests of a second party to protect that tender data which represents their business secret. Taking into consideration all the above, the Information Commissioner rejected the appeal of the applicant.

By way of its Decision No. 090-94/2009, of October 7 2009, the Information Commissioner ruled on the appeal of an applicant against a Decision issued by the Office of the State Prosecutor General of the Republic of Slovenia (henceforth: the VDTRS), by virtue of which the VDTRS rejected a request by an applicant to obtain copies of the 10 May 2009 recordings of surveillance cameras placed in front of the entrance to each floor used by the applicant and the VDTRS. Both the State Prosecutor General, Ms. Barbara Brezigar, and the former senior state prosecutor, Ms. Branka Zobec Hrastar, appear in the recordings. The VDTRS likewise denied the applicant access to the document by means of which the VDTRS regulates the handling and archiving of said surveillance recordings, as well as the VDTRS visitors book for 10 May 2009. The Information Commissioner established that all the security measures carried out for the purpose of protecting persons, documents and assets at the State Prosecutor's Office, are in the administrative domain of the State Prosecutor and thus also pertain to the of work of the VDTRS.

[15] Official Gatette of RS No. 42/2009, with amendments; ZGD.

Disclosure of the requested surveillance camera recordings, in accordance with Point 3 of Article 6 of the Personal Data Protection Act, represents the processing of personal data. The Information Commissioner furthermore emphasized, that in any implementation of Paragraph three of Article 6 of the Access to Public Information Act, one should differentiate between personal data which is directly related to the execution of public administration services, and the use of public finances by the state prosecutor as a public functionary, as well as all other personal data that the VDTRS manages as the controller of a personal data collection.

The Information Commissioner viewed the requested recordings and established that they did not depict any execution of public services by the two functionaries (Ms. Brezigar, and Ms. Zobec Hrastar) who appear in the recordings. Further to this appraisal the Information Commissioner did not establish any unreasonable use of public finances or irrational monitoring of the work of the VDTRS or indeed any irregularities in any procedures undertaken by the VDTRS. The Information Commissioner thus, on those grounds, rejected that part of the appeal by the applicant.

The applicant also requested insight into the VDTRS' visitors book for 10 May 2009, for which the Information Commissioner later established that that it included protected personal data (names and surnames of visitors who are not employed by the VDTRS) and unprotected personal data (personal data on civil servants employed with the VDTRS), and concluded that the VDTRS is obliged to provide the applicant with the requested document; however, protected personal data must be removed (redacted) beforehand.

The Information Commissioner established that the Rules regulating the procedures and measures for the protection of personal data during the video surveillance at entrances to official premises, are of an internal nature, and in this instance pertain to the internal workings and operations of the VDTRS rather than any public service provision. Disclosure of such data also partially reveals which parts of their VDTRS premises enjoy special protection measures as well as the characteristics of that protection. In the event that such data becomes freely accessible public information, then the efficacy of such protection may be voided, which would definitely disturb the operations of the VDTRS, because it can no longer proficiently protect its premises, hence the security risk increases. The Information Commissioner ruled that the VDTRS must conceal (redact) such data in the Rules, and submit the remaining part to the applicant.

By way of its Decision No. 090-162/2009/6 of 12 December 2009, the Information Commissioner ruled on the appeal against the decision of the Roads Directorate of the Republic of Slovenia (henceforth: DRSC) to charge an applicant for the re-use of information. The applicant had requested access to data from automatic traffic counter at the service *http://www.drsc.si/stevci/stevci_geors_si.xml*, which is fed via the Internet every fifteen minutes in the daytime and several times in the night time, 24-7. In such an instance it had to be clarified whether the applicant required such data for a commercial or for a non-commercial purpose.

The Information Commissioner established that the applicant shall re-use the requested public information in an XML format in such manner that all those who have access to the Internet may access - free of charge - this data via the GeoStik website. The service and the information would thus be accessible to everyone, with no limitations; however, the allure of said website would be increased as a consequence of such information provision, and any increase in visits to the site in itself would accordingly also increase its appeal and value to advertisers advertising on that website. Nonetheless, any such contention still does not represent the re-use of information for commercial purposes. On the basis of the above, the Information Commissioner granted the applicant's request and deemed that the DRSC should enable the applicant's re-use of the requested data, free of charge.

In its Decision No. 090-144/2009/8 of 27 November 2009, the Information Commissioner ruled on a complaint by a journalist against the office of the Attorney General in relation to

a failure to reply under the terms of the Media Act, to the following questions submitted by the journalist:

- How many expert opinions has the court expert provided the Attorney General over the past eight years?
- How much has the Attorney General paid the court expert over the past eight years?
- Has the expert issued an expert opinion on a given matter for the Attorney, and then issued another expert opinion on the same matter by order of the Court? Further to this last question: in which cases did this occur, and why did the Attorney General not take appropriate action.

The Information Commissioner established that replies to the applicant's questions pertain to expert opinions and subsequent assessments of expert opinions in relation to the procedures involving the Attorney General of the Republic of Slovenia before courts of law. The Information Commissioner has established that the Attorney General disposes of the documents which provide the answers to all the posed questions, save for that part of the final question as to why the Attorney General did not take appropriate action.

Save for one, all court proceedings, to which the applicant's request pertain, have now been completed, so that the exemption under Point 8 of the first paragraph of Article 6 of the Access to Public Information Act does not apply as regards the documents which are a part of already completed court proceedings. As regards the documents pertaining to ongoing court proceedings, the Information Commissioner has established that the harm which might result from implementation of the procedure has not been proven, so that these documents too do not represent an exemption under Point 8 of the first paragraph of Article 6 of the Access to Public Information Act. The Information Commissioner further establishes that the data pertaining to the name and surname of the court expert, together with the names and surnames of the attorney and the Attorney General, do not in themselves represent so-called protected personal data. Other personal data in the requested documents represents protected personal data and thus the Attorney General shall be obliged to provide the requisite documents to the applicant in such a manner that the protected personal data is concealed (redacted).

In its Decision No. 090-139/2009/5 of 17 November 2009, the Information Commissioner ruled on a complaint against the decision of the Ministry of Health to reject an applicant's request for the most recent draft proposal for the new Health Care Insurance Act (EVA: 2008-2711-0185), which is under preparation and is stated in the Government's 2009 Legislative Programme. The Information Commissioner has established that in this particular instance the exemption criteria under Point 9 of the first paragraph of Article 8 of the Access to Public Information Act were not provided, although the Ministry of Health stated they were.

The fact that a certain document merely represents a version of working materials and/or a proposal of a regulation does not mean that the actual given version of a document is - in itself - work in progress and something in the process of development. The version of the working materials in relation to the legislative proposal was created within the context of a working group, and unofficially communicated to bodies outside that working group, so the latter could communicate their opinions as to whether or not the suggested solutions presented an appropriate substantive direction.

The fact that the Ministry of Health had not yet marked the document as the final version of the proposal for the Health Care and Health Insurance Act is not reason enough in itself to deem it to be a document under preparation. In this instance, the draft represents an integral text of the working materials, prepared by a working group and the fact that this is most probably not the last version of the proposed legislation is also not relevant to this issue. Furthermore, the disclosure of this document cannot cause any incorrect understanding as to its content. The Information Commissioner hence imposed that the Ministry of Health allow the applicant access to the requested document.

By way of its Decision No. 090-137/2009/1 of October 1st 2009, the Information Commissioner ruled on a complaint in relation to an implied decision of the Agency of the Republic of Slovenia for Public Legal Records and Related Services (henceforth: AJPES), to which the applicant addressed a request for written explanations in relation to the following questions:

- Which act and/or data proves that the capacity of the company SGP Tehnik d.d. to settle its liabilities if below average?
- How was the calculation made (as regards content and actual figures) which led to the fact that the company SGP Tehnik d.d. was graded an SB6 credit rating?
- Which act and/or data prove that the company SGP Tehnik d.d. is under-averagely profitable, and that its liquidity is below average? What proof is there that the company has above average liabilities and below average assets and productivity?
- Which act and/or data prove that the company SGP Tehnik d.d. is more sensitive to changes in either operational circumstances or to changes in the business environment than an average Slovenian company?
- What is the basis of the comparison scale of erstwhile and present credit ratings (and which former rating is equivalent to the present rating)?

The disputed issue in this procedure was whether the requested information was within the jurisdiction (scope) of AJPES, which is subject to the provisions of Slovenia's Access to Public Information Act. On the basis of Articles 8 and 26 of the Decision on the establishment of AJPES (its constitution), the Information Commissioner established that AJPES provides services pertaining to the creation of credit ratings according to market principles, and thus the same rules apply to AJPES as they do to rating agencies operating under the tenets of private-law, to which the Access to Public Information Act does not apply.

The decisive fact in the decision in this case was that the information requested from AJPES by the applicant was not created in relation with the execution of AJPES' tasks and obligations under public-law, but rather in association with the execution of market activities and hence the information requested is not public information within the meaning of Article 4 of the Access to Public Information Act. Based thereon, the Information Commissioner rejected the applicant's complaint.

2.4. Overall Assessment and Recommendations Regarding Access to Public Information

2009 witnessed a significant increase in the number of appeals against the decisions of authorities of the first instance in relation to access to public information (182 appeals were lodged in 2009, up from 169 in 2008); complaints against implicit decisions also rose (302 in 2009, as opposed to 259 in 2008), as did requests for various explanations (328 in 2009, up from 102 in 2008). The number of requests for explanations reveals this area requires the more active involvement of Slovenia's Ministry of Public Administration, which, according to Article 32 of the Access to Public Information Act, is the ministry competent to deliver opinions and explanations. Practical dilemmas in this field are becoming evermore complex and demanding as regards their contents, hence first instance authorities need more assistance, guidelines and explanations in relation to the application of the provisions of the Access to Public Information Act. Indeed, this legislation imposes numerous obligations on a variety of organizations which, without adequate knowledge, financial and human resources, as well as the expert assistance from the responsible ministry, are unable to meet their responsibilities.

The Information Commissioner replied to all those who addressed a request for explanations, and in most instances it referred them to the competent institution. The Information Commissioner is namely an authority of second instance, which makes decisions in relation to lodged appeals. As such it is not competent to answer concrete questions as to whether or not a certain document is public information during the period in which an authority of the first instance is deciding upon that same case.

Based on actual appeal procedures, the Information Commissioner assesses that both the liable authorities as well as the applicants are today better acquainted with the various ways in which public information may be accessed. Indeed, said authorities are publishing significantly more public information on their websites, without any resort to requests by applicants. In 2009, the number of appeals in which the applicants were journalists and/or were lodged pursuant to Article 45 of the Media Act, increased significantly.

Those appeals being lodged with the Information Commissioner are becoming increasingly complex as regards their content and more voluminous as regards the number of documents that need to be deliberated. Most authorities are well acquainted with the practice of the Information Commissioner, because information on such is accessible via the Information Commissioner website. A well established practice has so been instigated in the field of access to information and such has also been endorsed by the decision of the Administrative Court, which handed down several important rulings in 2009 that exert a significant impact on the practice of first instance authorities as well as the Information Commissioner:

- In its ruling No. U 278/2008-23 of 20 October 2009, the Administrative Court adopted the position that appeals in relation to fees levied for access to public information shall be admissible, and that the appellate body in any such appeal shall be the Information Commissioner;
- In its ruling No. U 1410/2009-9 of 23 September 2009, the Administrative Court endorsed the Information Commissioner's position that the personal data of civil servants emanating from civil service inspectorate reports - i.e. in connection with their employment relationship and/or the use of public finance (e.g. data on workplace, title, salary, fulfilment of conditions for a certain position, data on promotion) should be freely accessible;
- In its ruling No. U 284/2008-35 of 27 May 2009, the Administrative Court adopted the position that in the event of any referral to business secrecy, parties must actually prove and substantiate that the legal provisions defining the existence of a business secret are fulfilled, and furthermore explain what actual damage or harm would be engendered or suffered through the disclosure of the particular information in question.

Although more than six years have passed since the adoption of the Access to Public Information Act, some liable authorities still perceive the tasks imposed on them by this legislation as additional work, rather than tasks under administrative law which they are legally obliged to carry out. In practice the Information Commissioner still observes that authorities perceive the Access to Public Information Act as a law which hinders them in carrying out their primary functions. As a consequence thereof, they transfer the burden of such tasks onto the applicants by charging fees for access to public information. It should be emphasized that the right of access to public information is a fundamental human right, enshrined in the second paragraph of Article 39 of the Constitution of the Republic of Slovenia, further to which the cost of access to public information should remain as low as possible and, therefore, must not disproportionally impede access. This is also supported by the provisions of Article 34 of the Access to Public Information Act which expressly provides that consultation at the source of the requested information shall be free of charge, and that the authority may charge the applicant material costs for the transmission of a transcript, copy or electronic record of the requested information. At present, the Decree on the transfer and re-use of public information is still problematic because it allows interpretation in the sense that it is possible to charge for the work that an authority renders in providing access to public information. Any such solution is also incorrect from a regulatory aspect, which is evident from the following:

- the General Administrative Procedure Act does not regard an authority's labour costs in conducting administrative proceedings, as a cost of those proceedings;
- according to the Administrative Fees Act, no administrative fees shall be levied for access to public information or for any appeal against the decision of an authority of the first instance, because any such procedure pertains to the exercise of a fundamental human right.

Consequential to all of the above, the Information Commissioner warns yet again that the non-critical, arbitrary and disproportionate levy of fees for the transfer of public information may actually jeopardize the entire public access system. The Information Commissioner thus advises against the use of tariffs or bills of costs that enable the arbitrary and uncontrolled charging of fees. Due to the inappropriate regulation of this whole issue, the Information Commissioner assesses that the institution of fees should be regulated differently in Decree on the transfer and re-use of public information.

It is a worrying fact that the number of complaints lodged against implicit decisions continues to increase. The Information Commissioner has observed in practice that liable authorities were forthcoming during many appeal procedures instigated as a consequence of their lack of response or reply in the first instance; it is arguably apparent that some authorities need more time than the twenty working days envisaged by the Access to Public Information Act. It should be emphasized that, in compliance with Article 24 of the Access to Public Information Act, in instances where an authority requires more time for the transmission of requested information, consequent to partial access to public information, or due to comprehensive documentation, it may extend the time limit by up to a further thirty working days, a measure which is seldom resorted to in practice, even in those instances where such may well be justifiable. Silence on the part of a liable authority is also unacceptable due to its responsibility towards applicants as well as towards the public at large. When lodging a request and receiving a negative decision, an applicant justifiably expects an explanation of the decision and such necessarily includes reasons for a refusal of access to information which would then enable the testing of that decision in the appeal procedure.

Yet again last year, the Information Commissioner failed to note any significant increase in appeal procedures in relation to the re-use of public information, the underlying reasons for which could be the economic crisis and consequent lack of applicant interest. Nonetheless, the Information Commissioner recommends that authorities pay more attention to the re-use of public information. This involves the propagation of public information, and its recycling by individuals and entities for both profitable and non-profitable purposes, this

with the exception of the original purpose of the performance of the public service for which the information and documentation was prepared in the first place. The utilization of information for the provision of a primary public service by an authority, or the exchange of information between bodies responsible for the performance of public services, shall not be considered the re-use of information. The re-use of public (sector) information involves its manipulation for commercial or non-commercial purposes, and results in its improved transparency and clarity. In the course of performing their mandated functions and services, public sector authorities collect, collate, reproduce and disseminate a great variety of information, the application of which - for purposes other than those for which it was originally intended - is considered as re-use. The aim of re-use is to gain additional value from public information, the private sector applicant should namely offer something else, additional or different from that which is being offered by the authority in the performance of its public mandate.

As for the commercial function, it vindicates the economic significance of public information, while the re-use of information results in the creation of a public sector information market, which is one of the key elements in dissemination by way of communication technology. Understanding the significance behind the creation of such a market is essential for the development of re-use. Commercial users, in particular, process public information, and, through the addition of new value, enrich it and offer it back to the market. It should be stated that it is the market alone - and not legislation - that facilitates the enrichment of information by commercial users. In accordance with paragraph 1 of Article 34a of the Access to Public Information Act, the public sector - i.e. every individual authority - is permitted to modify public information for the purposes of re-use. In effect this means that re-used information may be charged for on a commercial basis; however, such is not necessarily the case. It is also crucially important to ensure that there is no discrimination among applicants, i.e. the re-use of information shall be permitted by all applicants, at the same price and under the same conditions. Considering the beneficent effects of re-use it would indeed make sense for the liable authorities to begin promoting it. Besides which, the provision that determines certain information should be published by the liable authority, in advance, via the Internet, must also be respected. Accordingly, all conditions for the re-use of information, the usual price, as well as the calculation basis for charging for re-use in instances of specific requests, must be published on the web.

3 ACTIVITIES IN THE FIELD OF PERSONAL DATA PROTECTION

3.1. Concept of Personal Data Protection in the Republic of Slovenia

The concept of personal data protection in the Republic of Slovenia is predicated on the provisions of Article 38 of the Constitution of the Republic of Slovenia. According to this provision, personal data protection is one of the constitutionally enshrined human rights and fundamental freedoms. The provisions of Article 38 of the Constitution of the Republic of Slovenia ensures the protection of personal data, prohibits the use of such data in a manner contrary or beyond the reason(s) and purpose(s) for which it was collected; furthermore, it facilitates the right of access by the individual to collected personal data which refers or pertains to them, in person, and includes the right to protection under law for anyone whose personal data has been misused. Particularly important with regard to the normative regulation of personal data protection is the second paragraph of Article 38 of the Constitution of the Republic of Slovenia, where it is specified that the collection, processing, application, supervision, protection and confidentiality of personal data shall be regulated by law. By way of this, the legislator has decided upon the enactment of the so-called »processing model« as opposed to the so-called »model of misuse«, since legislation has primarily specified admissible personal data processing and not freedom based on principles regarding personal data processing that can only rarely be explicitly constrained by law. In accordance with this model, everything in the field of personal data processing, except that which the law explicitly allows - and in the private sector that which may be also mandated through the provision of explicit consent by the individual - is prohibited. Each instance of personal data processing is a sign of the encroachment of the individual's constitutional right to the protection of their personal data. Thus such intervention is allowed only if the law explicitly specifies exactly what personal data can be processed, and additionally clearly defines the purpose of processing personal data, as well as provides adequate protection and security of the personal data. Only those elements and aspects of personal data that are appropriate and strictly necessary to realize certain specific legally defined and constitutionally admissible functions and purposes may be processed.

The Personal Data Protection Act[16] was adopted by the National Assembly of the Republic of Slovenia on 15 July 2004, and has been in force since 1 January 2005. Adoption of this Act was for the most part a consequence of the accession of Slovenia to the European Union, and the resultant obligations to harmonize personal data protection with the provisions of Directive 95/46/EC of the European Parliament and the Council for the Protection of Individuals regarding Personal Data Processing and the Free Movement of Such Data[17].

In July 2007, amendments to the Personal Data Protection Act were adopted by way of the Act Amending the Personal Data Protection Act[18]. This legislation introduced two important novelties, namely from the perspective of the administrative and - as a consequence thereof - the financial disburdening of those responsible for administrating personal data as well as prescribing certain relief as regards the methods by way of which individuals may access their own personal data. The amended legislation significantly narrowed the circle of persons liable for the entry of personal data collections into the register, and also brought a number of positive solutions, in particular relief for individuals to whom personal data relate, regarding the ways they may access personal data that pertain to them. Official consolidated text of the Personal Data Protection Act has been published in September 2007.

16 Official Gazette of RS No. 86/2004.
17 Official Journal of the European Union, No. L 281, 23rd November 1995.
18 Official Gazette of RS, No. 67/2007.

3.2. Review of the Activities in the Field of Personal Data Protection in 2009

During 2009, the Information Commissioner received 624 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act; namely 219 in the public sector and 405 in the private sector. There were 165 applications and complaints against public sector legal entities, 54 procedures were initiated ex officio; whereas 332 applications and complaints were made against private sector entities, and 73 procedures initiated ex officio. Statistical data indicates that the number of applications as to alleged violations of Slovenia's Personal Data Protection Act remained at almost the same level as in 2008. Following assessment of the received applications and ex officio cases, 124 inspection procedures were initiated in relation to public sector entities, and 267 in private sector entities. 298 physical inspections were carried out in the scope of inspection procedures. On the basis of Article 33 of the Inspection Act[19], 66 cautions were issued in relation to minor irregularities. 47 regulatory and administrative decisions were also handed down, whereby the liable persons were ordered to undertake measures to rectify the established irregularities. 338 inspection procedures were concluded with a decision to stay the proceedings.

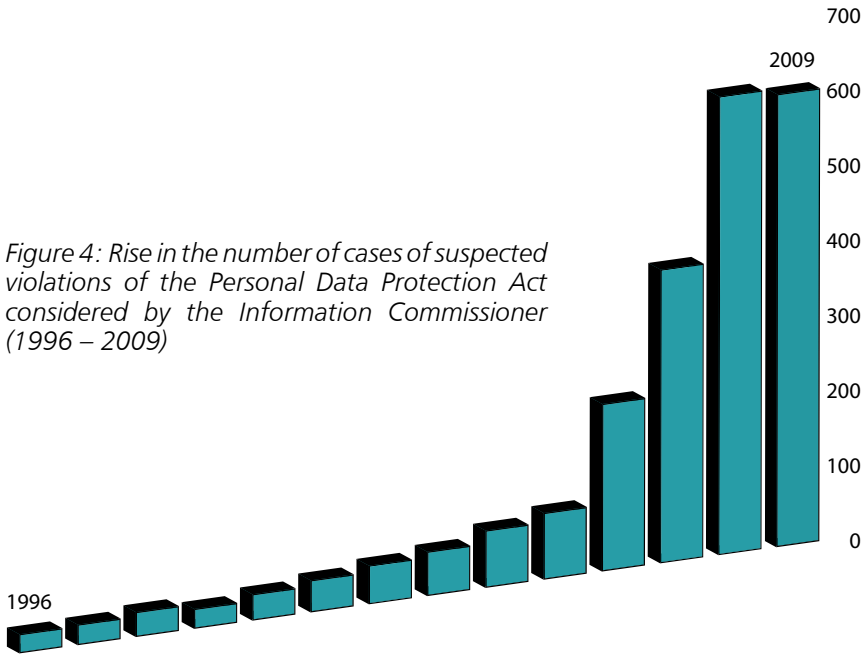


Figure 4: Rise in the number of cases of suspected violations of the Personal Data Protection Act considered by the Information Commissioner (1996 – 2009)

In 2009, most cases of suspected violations of the Personal Data Protection Act pertained to:

- illegal collection or request for personal data (134 instances);
- disclosure of personal data to unauthorized users by a personal data collection controller (110);
- illegal publication of personal data, for example on notice boards and in the media (77);
- illegal video surveillance (57);
- insufficient security measures to ensure adequate protection of personal data (54);

19 Official Gazette of RS, No. 43/2007 - official consolidated text 1; ZIN.

- misuse of personal data for the purpose of direct marketing (38),
- other issues; such as illegal implementation of biometrics,
- as well as the processing of personal data in a manner discordant with the purpose for which it was collected (27).

Figure 5: The relative number of cases of suspected violations of the Personal Data Protection Act considered by the Information Commissioner in 2006-2009

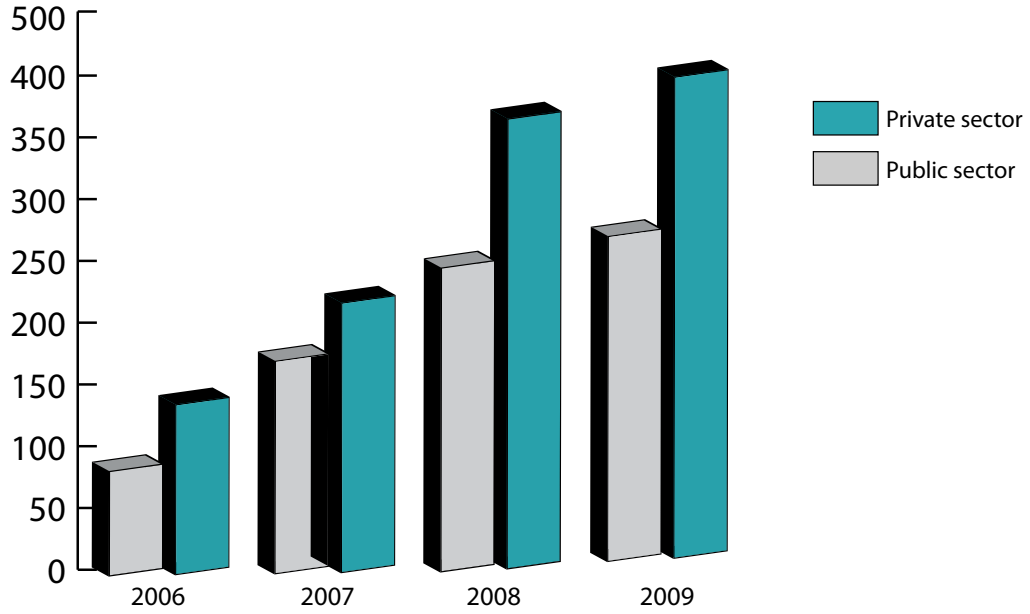
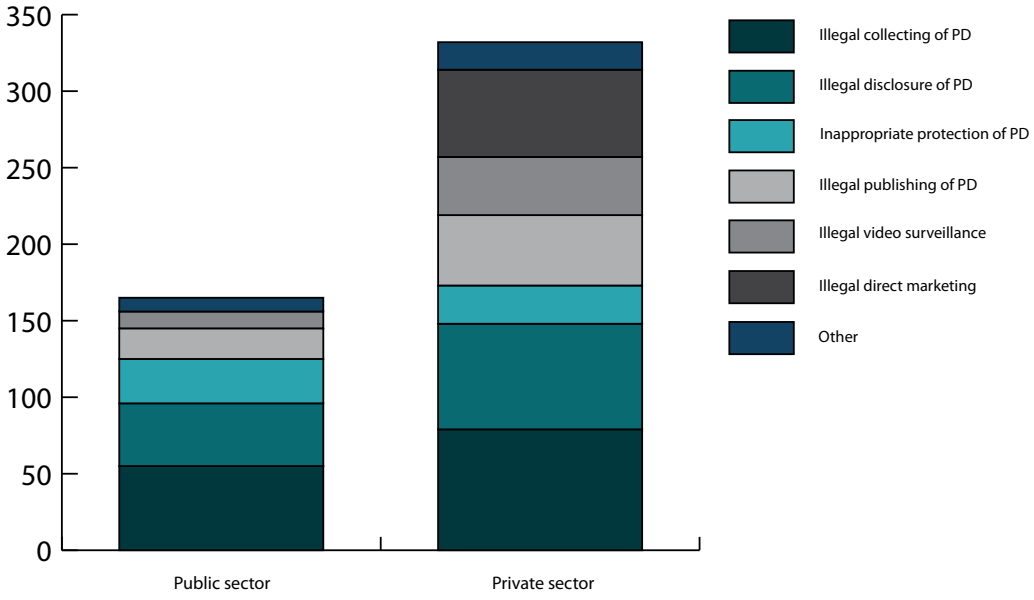


Figure 6: The illegal processing of personal data in 2009 as identified by the Information Commissioner: a comparison of the public and private sectors.



163 violation procedures were initiated in 2009 as a consequence of violations of the provisions of the Personal Data Protection Act; these were namely: 41 procedures against public sector entities, 70 against legal entities in the private sector, and 52 procedures against individual persons. Violation proceedings are considered in accordance with the Personal Data Protection Act. As a consequence of established violations, the Information

Commissioner issued:

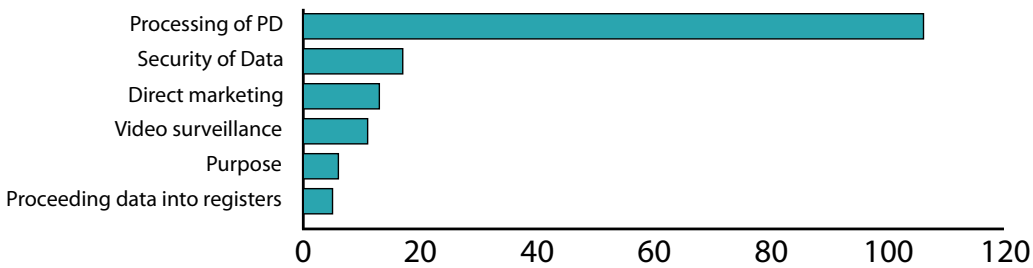
- 59 warnings (seven in proceedings initiated in 2008),
- 93 decisions regarding violations (encompassing 67 cautions, thirty thereof in relation to proceedings initiated in 2008; as well as 26 fines, nine of which pertained to proceedings initiated in 2008),
- 12 payment orders

In 2009, 21 offenders lodged applications for judicial protection; 16 against fines, and five against cautions.

In 2009, the Information Commissioner received 14 judgments, where local courts heard applications for judicial protection from the rulings handed down by the Information Commissioner in recent years. The judgments of these courts were as follows:

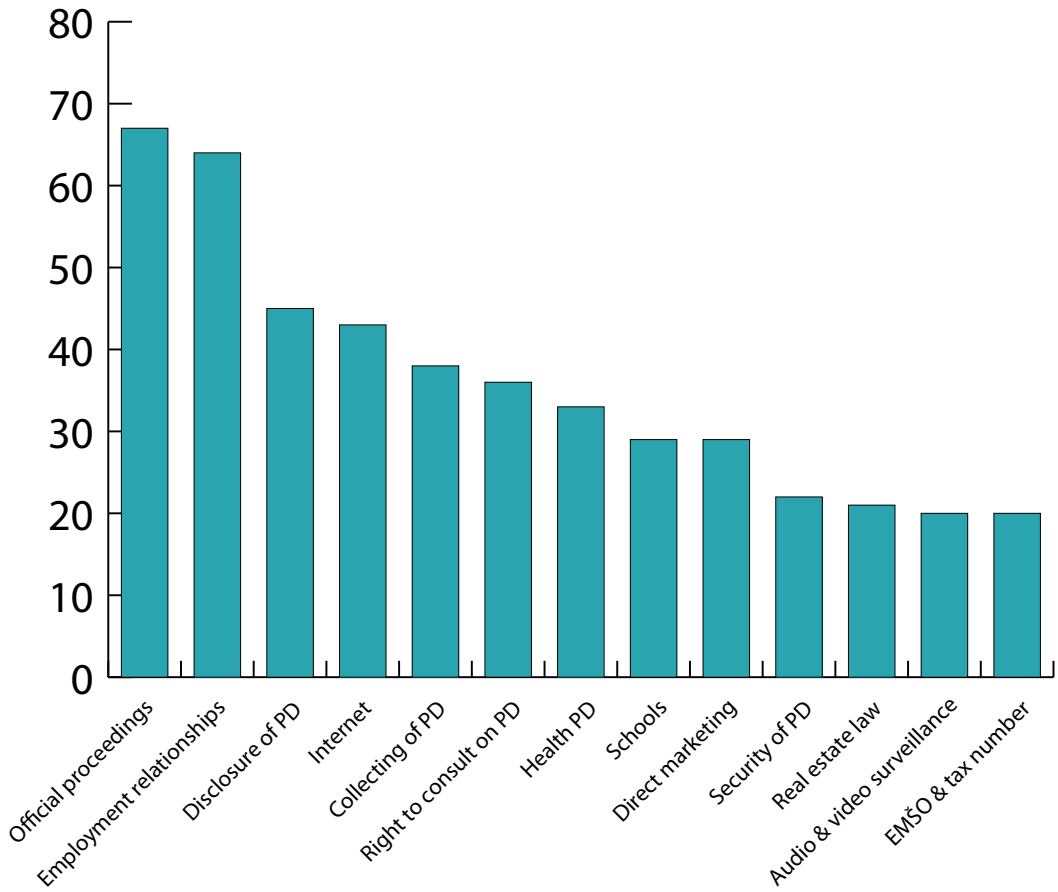
- the application for judicial protection was refused and the ruling of the Information Commissioner was upheld in nine instances;
- the application for judicial protection was granted in that part which pertains to the imposition of a sanction, thus the sanction was amended, however, the request for judicial protection in relation to the ruling was refused in three instances;
- the application for judicial protection was granted, the Information Commissioner's ruling was stricken, and proceedings in relation to the offence were stopped in two instances.

Figure 7: The most common violations of Personal Data Protection Act



In 2009, the Information Commissioner received 1334 requests for written clarifications or opinions regarding specific issues, which is over fifty percent more than in 2008, when the Information Commissioner received 853 such requests. The requests for opinions and clarifications are becoming more demanding as regards their content, which can be ascribed to the fact that public awareness of the Personal Data Protection Act – and the rights of the individual that are afforded by it – is becoming ever greater. The Information Commissioner issued 596 written opinions and clarifications for those more demanding questions which as yet have not been addressed by the Information Commissioner in the history of its operations; those persons who posed questions to which the Information Commissioner had already replied in the past, were referred to the already issued opinions. There were 738 such referrals and recommendations pertaining to the Personal Data Protection Act. The Information Commissioner also provided oral opinions and clarifications. An Information Commissioner employee is on-duty from 8 a.m. to 4 p.m. every day to answer telephone enquiries.

Figure 8: Requests for the Information Commissioner's opinion in 2009: by area (a single opinion may relate to different areas).



The Information Commissioner received 40 applications concerning the implementation of biometric measures during 2007, 16 applications in 2008, whereas in 2009 it received just ten such requests, which means that the number of such applications is decreasing. Six decisions as to the admissibility of biometric measures were issued in 2009, of which two had been lodged in 2008; one application was withdrawn by the applicant. Four decisions vindicated the implementation of biometric measures; limited implementation was approved in three instances, while two decisions explicitly proscribed the introduction of biometric measures.

Affirmative decisions were granted to those legal entities where it was established that biometric measures were vital to the performance of activities, the safety of employees and property, as well as the protection of classified information or business secrets. The Information Commissioner accordingly permitted the implementation of biometric measures upon the employees of a bank, namely by means of biometric devices which operate on the principle of face recognition, and which are located at the entrances to its computer centres and strong-rooms. The Information Commissioner also permitted the implementation of biometric fingerprint readers for the identification of employees entering premises containing classified information within the Permanent Mission of the Republic of Slovenia to the European Union in Brussels. The introduction of biometric fingerprint readers was also allowed at the entrance to the office of the managing director of a transport and logistics enterprise, this for the purpose of protecting the business secrets held within, as well as at the entrance to premises owned by a telecommunications

operator which deals with system administration and business solutions. In the second of these applications biometric control measures were used at the entrance to a safe room as well as for unlocking of cabinets in which the information-communication equipment is located on which the company's most sensitive information - including personal data pertaining to personnel, medical data, business secrets, classified information and archive materials - in relation to its various clients - among which are state authorities, public institutions and corporate clients - is electronically stored using the company's so-called siHramba application.

Refusals were issued to applicants who looked to implement biometric measures merely to record working hours or attendance, for the reason that such a system would be more practical than using contactless cards, or merely because an employer wanted to prevent abuse through one employee lending a card to another. Such reasons do not justify the implementation of biometric measures, and in themselves would constitute an excessive and unnecessary violation of employee privacy, given that registering attendance can forever be undertaken in a less intrusive way.

During 2009, the Information Commissioner received seven applications for the export of personal data. It issued six decisions, one of them in relation to an application received in 2008. All applicants who received decisions were permitted to export the data. These were as follows:

- The Information Commissioner received a proposal from a company engaged in graphic and documentary services, which also owns an enterprise in the Republic of Croatia, to instigate a procedure to assess the suitability of the personal data protection regime in the Republic of Croatia, for the reason that the transfer of some personal data from one of company to the other would be unavoidable in the execution of business operations. Upon the investigation procedure, the Information Commissioner concluded that the Republic of Croatia provides an entirely appropriate level of personal data protection.
- The Information Commissioner allowed a company engaged in the production of transport devices to export and transfer personal data on its employees to contractual personal data processors in third countries, namely to the USA, India and Egypt for the purpose of human resources and applications support, as well as logistics system support related to proposals, the implementation of contracts and supply of products, for the establishment and maintenance of email systems and pertaining hardware, as well as for the purpose of asset management and system maintenance at the desktop and network levels.
- The Information Commissioner allowed a management consulting company, which is a member of an international network of companies, to export and transfer to their contractual processors of data in third countries (importers of data in the USA and Singapore). The exported data pertains to personnel (of the company and third-party enterprises) and shall be stored in data centres (servers) which shall enable data access to members of an international network of independent companies.
- The Information Commissioner authorized an auditing company, which is a member of an international network of companies, to transfer and export data pertaining to its employees and third persons, whose data is also in its possession, to its contractual processors of personal data in third countries (the USA and Singapore), for the purpose of server storage.
- The Information Commissioner authorized a company marketing medicines to transfer and export data pertaining to its employees and third persons, who have access to the company's information systems, as well as data on clients, suppliers and other persons, whose data the company stores, to their contractual processors of personal data in third countries (namely, the USA, South Africa and India), for the purpose of providing information services within the scope of its Help-Desk Server together with remote access technical support via the desktop.
- The Information Commissioner authorized a legal entity engaged in manufacturing, development and sales to transfer to companies within a certain business group in the USA, personal data pertaining to its employees, contractors and students for personnel purposes and in order that its operational performance would be improved.

The Information Commissioner received five applications for permission to merge personal data collections during 2009. Eight positive decisions - five of which were issued in relation to applications lodged in 2008 pertained to the granting of permission for the merging of one data collection with one or more other data collections (e.g. the direct computer connection of a waiting list with the Central Population Register; the direct computer connection of the Compulsory Health Insurance Register with the Central Population Register within the scope of the e-Rojstvo ("e-Birth") application; the merging of three collections of personal data: Medical Records, the Central Population Register and the Civil Register; the merging of the Central Electronic Data Storage (CEH), the Central Population Register, the Tax Register RS, the Slovenian Business Register and the Compulsory Health Insurance Register all within the e-VEM information system; creating a direct computer connection between the List of Controllers and the Central Population Register; the merging of the National Population Register and the Household Database; the merging of the following data collections: Central Register of State and Public Sector Non-Financial Assets, Land and Cadestral Register and the Property and Deeds Register; as well as the merging of the Dogs Register and National Population Register.) The common denominator in all but one instance of merger was the EMŠO - Slovenia's system of unique personal identification numbers issued to all citizens; in the other instance the common element was the tax number. Mergers and exchanges involving personal data collections are only permissible as regards certain types of personal data determined by law.

During 2009, the Information Commissioner received 70 complaints with regard to the right of citizen's familiarization with their own personal data, which reveals that the number of complaints is still increasing. Most were in relation to healthcare institutions as well as employees, courts, ministries and bodies affiliated to ministries. 57 of the received applications were addressed. In 23 instances the data controllers disclosed the data immediately upon receiving a call from the Information Commissioner, in three instances data controllers were obliged by the decision of the Information Commissioner to allow the applicant access to their own personal data; 12 applicants were referred to the competent institution and/or were given advice as to what procedure to follow, seven applicants withdrew their complaints, and 11 individuals received explanation as to why their applications did not represent a complaint as regards refusal to access their own personal data and/or that their complaint was not substantiated. In one instance infringement of the provisions of the Personal Data Protection Act was established and consequently an inspection was instigated.

3.3. Major Violations of Personal Data Protection

Illegal Collection of Personal Data on Potential Voters by Political Parties

Last year, the Information Commissioner instigated an inspection procedure as a consequence of the suspected illegal collection of personal data on potential voters abroad for the purposes of direct marketing in the relation to Slovenia's parliamentary elections. The Information Commissioner became attentive of the infringements when it received several applications from citizens living abroad, who also enclosed such political propaganda materials with their letters of complaint. Within the scope of the inspection procedure, the Information Commissioner established that two political parties were not able to provide proof of any legal basis for the collection and storage of the addresses of Slovenian voters abroad.

It was established during the inspection procedure, that some sympathizers abroad supplied a number of names and addresses to political parties, while those identified individuals were not made aware thereof. Any such database was collected and established within the understanding of the provisions of Item 4 of Article 13 of the Personal Data Protection Act and with reasonable intentions - they were pursuing a legal activity in accordance with

their political goals. They apparently did not want to cause any damage or harm by sending the political materials, and ultimately gained little benefit from the exercise, because the political parties in question failed to obtain any seats in parliament. Both political parties namely collected and processed personal data on the basis of Item 4 of Article 13 of the Personal Data Protection Act. This Article provides a legal basis for political parties to process personal data on individuals; however, such data must have been obtained legally. Both political parties and the respective responsible persons were sanctioned within the scope of proceedings in relation to failure to comply with the provisions of Article 8 of the Personal Data Protection Act.

Illegal Personal Data Collection on Telephone Conversations

During the inspection procedure, the Information Commissioner established that an official at a District Court collected personal data on telephone calls made using a mobile phone which is the property of the Court and used for Court business. The official's actions were neither sanctioned nor legal, and the data obtained was processed in a manner which was not in compliance with the purpose for which it was originally collected. The data on telephone calls from a corporate mobile phone was not obtained on the basis of a complaint in relation to bill correctness, as set forth in Article 9 of the Rules for using mobile phones and other mobile telephony services, but for obtaining personal data in relation to the calls made using the apparatus (i.e. the date and times of calls, telephone numbers to which calls were made or text messages sent, duration of calls, as well as the type and amount of the services provided) in the form of an itemized bill provided by the operator Mobitel d.d.. The data on telephone calls was obtained with the purpose of documenting the course of the mutual exchange of information on a bomb explosion at the home of Judge Katarina Turk-Lukan, and then to further process and use such data to establish which person at the District Court communicated with journalists using the mobile phone.

As a consequence of its inspection procedures and subsequent findings, the Information Commissioner imposed a sanction on the responsible person at the District Court, in relation to two offences of illegal personal data processing (contraventions of Article 16 of the Personal Data Protection Act). The Decision of the Information Commissioner is not yet final.

This case is yet a further illustration of the pressing problem of legal irregularities in relation to privacy in workplace in the Republic of Slovenia. The Information Commissioner has provided warning thereof on a number of occasions; indeed, one-third of cases related to the protection of personal data pertain to this same problem.

Processing the Personal Data of Insured Persons by Insurance Companies without any Legal Basis or Personal Consent

Last year the Information Commissioner decided on yet another case pertaining to the illegal processing of personal data in relation to two insurance companies, an incident which attracted a deal of media attention. The inspection procedure revealed that personal data in relation to 2382 erstwhile insured persons had been transferred, without any legal basis or the consent of the individuals to which the data pertained.

In the context of this procedure, the Information Commissioner imposed sanctions - against the insurance companies and the responsible persons - for illegally processing personal data. The Information Commissioner levied fines as a consequence of the unlawful collection and transmission of personal data pertaining to 26 individuals, for whom conclusive evidence has been provided, as well as for making such data available and not providing any traceability as to the transfer itself. One insurance company lodged an appeal against the Information Commissioner's ruling and requested judicial protection; the other insurance company has settled one half of the imposed fine, and formally appealed in relation to the remainder.

The fines are the highest ever imposed by the Information Commissioner. Further to this, the Information Commissioner wishes to signal its future intent to heavily sanction the illegal transfer or sale of personal data, especially in relation to data controllers who manage large collections of personal and sensitive personal data.

Illegal Insight into the Personal Data of Bank Customers

In 2009, the Information Commissioner carried out systematic control over the protection of personal data within Slovenia's banking sector, within the scope of which the Information Commissioner made assessments as to the legality of the processing of personal data in relation to the access of data on private bank accounts, the provision of credit ratings and the inter-bank exchange of data on customers, particularly in relation to the newly established SISBON system. No illegal procedures were detected in relation to the inter-bank exchange of data on the credit ratings of customers.

During verification as to the access of confidential banking data pertaining to some well-known Slovenians, it was established that personal data had been illegally accessed at two of the country's six largest retail banks. The Information Commissioner imposed sanctions in accordance with the General Offences Act, due to a failure to observe the provisions of Article 8 of the Personal Data Protection Act.

Publication of a Journalist's Questions and E-mail Address

The Information Commissioner published on its website, as well as distributed to a larger number of addresses, a facsimile of an email it had received from a journalist which posed a number of questions for address by the Information Commissioner. As a direct consequence of this publication, the journalist lodged an application in relation to the Information Commissioner's violation of the Personal Data Protection Act. The Information Commissioner did not instigate an inspection procedure in relation to this complaint, and established that in this instance no offence had been committed.

The published email address, via which the journalist's questions was sent, was a corporate address provided by the journalist's employer; the email was addressed to the official electronic address of the Information Commissioner, to which legal and natural persons send emails in relation to matters pertaining to the work of the Information Commissioner. In this instance, the name and the surname, together with the email address of the journalist who had posed the questions, do not represent protected personal data, because the journalist was carrying out his journalistic function, and his name and surname are publicly published on the website of the company he works for.

The content of the electronic mail, in combination with the name of the person does indeed represent personal data within the meaning of Article 6 of the Personal Data Protection Act; however, the provisions, set out in Item 3 of the first indent of Article 6 of said Act provides that not all personal data has at the same time the status of protected personal data, and/or that personal data disclosure is - in certain instances - admissible, if it constitutes the exercise of the right of access to public information.

The journalist's privacy and dignity (protected under Article 1 of the Personal Data Protection Act) were not violated by publishing his electronic address. The Information Commissioner simultaneously established that the email containing the journalist's questions were not of a personal nature, but they rather pertained to the public function of the Information Commissioner.

By its very nature, the content of a written communication which is intended for publication in the media cannot be protected as private; as such it represents public information. The publication of the content of the journalist's email on the Information Commissioner's

website did not represent a violation, because in this instance the data was not personal, and thus not protected within the terms of the provisions of the Personal Data Protection Act.

Publication of Court Judgment in a Newspaper

As a consequence of a Slovenian daily newspaper publishing part of a court judgment, which contained personal data in relation to a plaintiff, the Information Commissioner established an infringement of the provisions of the Personal Data Protection Act and imposed a sanction on the newspaper company and the responsible person. This case is significant because the Information Commissioner took the position that the personal data, stated in the judgment, which pertains to a non-public person, represents protected personal data, consequential to which the judgment should only have been published in an anonymized form. In this case, at the collision of two constitutional human rights - namely, on one side, the right of expression and the related constitutional principle of the public nature of a trial, and, on the other, the non-public person's right to the protection of their personal data - the Information Commissioner took a clear position that in compliance with the principle of the limitation of human rights and fundamental rights by the rights of others, the right to the protection of personal data prevailed over the right to fully publish the decision of a court.

Public interest, with regard to the provision or publication of information which merely satisfies curiosity, cannot in itself be the justification for an encroachment into the information privacy and/or the constitutional right to the protection of personal data of an individual who is not in the public eye.

3.4. Overall Assessment and Recommendations in Relation to the Personal Data Protection

Observations in 2009 revealed the same and similar violations and irregularities pertaining to personal data protection as had been the case in previous years.

Among the most common are misdeeds pertaining to the maintenance and administration of personal data collection catalogues, as well as the relation of such to the Information Commissioner, the body responsible for managing the register of personal data collections. In relation thereof, we would like to expressly emphasize that many controllers of personal data do not take sufficient care as to the accuracy and update of the data in their personal data collection catalogues, and thus the register of personal data collections is deficient.

Consequent to its inspection procedures in relation to video surveillance, the Information Commissioner establishes that such surveillance is increasing year by year; however, the most common irregularities in relation to video surveillance remain the same. Transgressions are mainly manifested in deficient notifications as to surveillance - i.e. they do not include all the information prescribed by law, or were too small in size and displayed in inappropriate places - as well as the failure to provide written notification as to any decision to instigate video surveillance as well as adequate reasons for its implementation. Deficiencies in maintaining records of the inspection of recordings are also apparent.

In the realm of direct marketing, it was ascertained that data controllers not only use contact data (name, surname, telephone number, fax number and e-mail address) for which they do not need personal consent - providing that such has been obtained from publicly accessible sources in the pursuit of lawful activities - but they also use other personal data (e.g. data as to the value of their property or data on shopping habits) without first obtaining the personal consent of the individual concerned. Further to this, the direct marketers often

failed to inform the individuals they contacted as to their statutory right to demand - at any time, by way of a written request or indeed in any other manner - that the data controller desist from the use of their personal data in direct marketing activities.

In 2009, the Information Commissioner established many irregularities in relation to the contractual processing of personal data. According to the provisions of Article 11 of the Personal Data Protection Act, the controllers of personal data may entrust individual tasks related to the processing of personal data to legal entities or natural persons who are registered to perform such activities. However, controllers often forget that they must conclude a written contract with these contractual processors, which, in addition to clear authorization for the processing of personal data, must contain an agreement on the procedures and measures pertaining to the protection of personal data, further to which the data controller shall oversee the implementation of procedures and measures pertaining to the protection of personal data.

In relation to the execution of measures and procedures for the protection of personal data under Article 24 of the Personal Data Protection Act, warning is made that the circle of employees who have access to certain personal data administered in an individual collection, is often too broad and, furthermore, the Information Commissioner often establishes deficient traceability, or even an absence of traceability, in the processing of personal data.

Last year the Information Commissioner yet again dedicated a deal of attention to the question of employee expectations of privacy in the workplace, especially related to the use of corporate email, telephones and computers that are - to at least some extent - also used by the employees for private purposes. Such use indeed represents a conflict of interests. Employers enjoy the right of ownership over their assets, and consequently the right to control whether such assets are used in accordance with the purpose for which they were provided; at the same time, individual employees are also entitled to expect some degree of privacy and confidentiality in the workplace. Through its involvement in such cases, it is evident to the Information Commissioner that the sphere of privacy in the workplace is under regulated, further to which it has provided a number of warnings to this effect. In order to resolve various dilemmas, the Information Commissioner last year prepared a draft for a Communication Privacy in the Workplace Act, the purpose of which is to set forth principles and conditions in relation to intrusions into the communication privacy and dignity of employees in their use of a telephone, computer, the Internet, email as well as other means of communication in workplace. Said legislation would also regulate company car usage and the processing of locational data in relation to employees whereabouts. The Information Commissioner has already submitted a draft of the projected bill to Slovenia's Ministry for Labour Family and Social Affairs; however, no further action has - as yet - been taken.

Privacy is often exposed in the context of the information society. Transition from analogue to digital, and, with that, from manual to the mechanical, have engendered unforeseen possibilities in the ultra-rapid collection and processing of huge amounts of personal data. In the context of modern society, privacy is in competition with the economy; and in order to maintain privacy, pressure must necessarily be exerted from the aspect of the consistent application of systematic information security. When there is a general failure to provide, ensure or uphold such systems - as is especially evident in relation to the Internet - privacy loses the battle.

The Internet is by all means mass media; it has experienced a tremendous degree of development over the past decade as well as exerted a major impact on privacy. Indeed, only recently Google celebrated its 10th anniversary, whilst Facebook, the world's largest social network, is not even five years old; there are many people, however, who could not envisage their everyday lives without such utilities. We are probably not even aware as to how much data these giants have on us. If someone were, for example, to intensely use a broad spectrum of Google services - email, browser, on-line maps, news readers, calendar,

clipboard, social network, direct messaging and so on - Google would probably know more about them than any other person or institution. Google would know what you sought on the Internet, which sites you visited, who your friends are and what you talk about with them. If we wanted to compare this to the real world, the only person who could collect such all-embracing information about you would be a little gnome sitting on your shoulder and monitoring everything you do. Any such elf would, of course, log this information electronically making it ideal for further processing.

Further to this ongoing battle between information privacy and the highly acquisitive tendencies of commerce, privacy invariably competes with increasingly frequent and radical security measures. One of the most recent of these are body scanners, by means of which authorities intend to apprehend potential terrorists carrying weapons or explosives on their person. The protectors of security are probably unaware as to the broader consequences that the potential actions of a single individual has on us all. Today everyone is subject to body imaging at airports, thus such measures are a mere security theatre that has the appearance of providing additional security. Surely in relation to such blanket screening, potential terrorists shall simply redirect their attentions to alternative means or other targets. At the same time the question arises: how come similar such measures are not being implemented at other mass events?

The question remains: how shall we balance measures aimed at increasing general security against encroachment into our privacy and even the freedom of us all? The answer may well lie in the implementation of technology in such way that it shall increase the level of security and at the same time minimize encroachments into the privacy of the individual. Amongst Ombudsmen and Information Commissioners there is much talk about so-called Privacy by Design - an approach which endeavours to minimize the amount of personal data processing necessary to achieve legitimate and legal objectives. This approach utilises technology that facilitates a positive sum game, whereby an increase in the level of security provision does not involve any sacrifice of privacy. By way of such an approach, the scope of encroachment has to have been taken into consideration in the initial phase of the security technology concept. As for body imaging – and providing its implementation is really necessary, effective and proportional to their encroachment upon the privacy of the individual – the technology should only enable the depiction of no more than is strictly necessary.

The overall conclusion is that the preservation of privacy is still possible even with the most intrusive measures; nevertheless, such protection forever requires effort, knowledge, resources, as well as the will, to accomplish. Without all of the above the fight for privacy is - alas - all too frequently lost.

Significant developments are also occurring in the domain of direct marketing. There is an increasing amount of profiling and behavioural targeting, where consumer profiles are created on the basis of personal data collection and the marketing is specifically targeted on the basis of the profile developed through data processing. Such profiling is further emphasized and enhanced through the issue of loyalty cards and clubs, and such also extends to electronic communication and the Internet. Digital television, for example enables monitoring as to who is watching which channel. Providers are thus able to create individual viewer profiles of their audiences on the basis of which advertising may also be specifically targeted. In effect this means that in future different households and content consumers will be subjected to different commercials, and then we will genuinely be able to ask ourselves: Who is watching whom? Are we watching TV, or is the TV watching us? Such experiments are already well underway via the Internet (the digital technology company Phorm is well known in this field), while technologies for the supervision of the Internet (such as deep packet inspection) employed by Internet service providers, and used by technology companies for the benefit of advertisers, have already established a significant presence, which is surely destined to become ever stronger and more developed.

Until recently advertisers placed advertisements in relation to content provision, in much the

same way as they did in conventional media; in an era in which Internet service providers are able to create consumer profiles based on an individual's use of the Internet, ISPs are in a far stronger position in relation to the provision of advertisements specifically adapted to the individual's behavioural profile. An analogy in the physical world would be a postman who opens your mail, reads it, and is ultimately in a position to enclose an appropriate advertisement within, before delivering you your letter. In the light of such comparisons, the ultimate legality and constitutionality of such actions become more explicit.

As regards personal data protection in Slovenia's healthcare sector, the Information Commissioner is still receiving a great many complaints, most of which pertain to the inappropriate protection of sensitive personal data. In its inspection procedures, the Information Commissioner frequently establishes that health service providers have not even provided the basic elements of security, such as regulated access authorizations to data, and all too frequently they do not even have transparent or supervised business processes; thus the issue of traceability in personal data processing is ever more pressing.

The absence of some fundamental elements in information security is reflected in the lack of ability to establish, apply or prove responsibility for the misuse of personal data; such is also manifest in the unintended processing and transmission of personal data to unauthorized third parties. A change in attitudes to personal data protection is necessary in the health sector, as is the implementation of integrated systematic approaches to the protection of information based on internationally established standards, such as ISO/IEC 27001. Taking into consideration the aforementioned, and in light of the protection of personal data (further to Article 14 of the Personal Data Protection Act), changes in legislation should also be considered in order to raise the level of requirements of data processors.

The Information Commissioner has been facing numerous dilemmas in the realm of telecommunications, particularly so in the area of compulsory retention of data on electronic communications. Some ex officio inspections specifically carried out in this area reveals that that protection of stored data is for the most part appropriate; however, a number of smaller telecommunications operators are exhibiting more severe deficiencies.

The Information Commissioner assesses the impact of the General Act on the Secrecy, Confidentiality and Safety of Electronic Communications, the Retention of Data and the Protection of Stored Data[20] - which sets forth strict standards of information security in this sector - most positively. Nevertheless, there are still numerous predicaments as regards access to stored data, and thus the Information Commissioner takes the position that the provisions of Slovenia's Criminal Procedure Act and the Electronic Communications Act should be aligned in order to avoid disparate interpretations; further to this, a number of measures in relation to the regularisation of authorizations have already been implemented in conjunction with the Ministry of the Interior. The Information Commissioner warns as to the absence of a platform which would enable a better co-operation and the exchange of expertise between itself, the Ministry of the Interior, the Post and Electronic Communications Agency of the Republic of Slovenia, authorities, law enforcement agencies, operators and solutions providers active in the field of data retention.

In 2009, the Information Commissioner imposed it highest fine to date; this was in relation to two insurance companies as a consequence of the illegal processing of personal data. The proceedings established that personal data pertaining to 2,382 former insured persons had been transferred from one insurance company to the other without legal basis or the personal consent of the individuals concerned; the data thus transferred was then used in direct marketing. The Information Commissioner imposed a EUR 112,590 fine on the provider insurance company for the illegal transmission and non-traceable dissemination of personal data pertaining to 26 individuals, in relation to whom firm evidence had been provided; a EUR 20,000 fine was imposed on the responsible individual. The recipient

[20] Official Gazette RS No 126/2008.

insurance company received a fine of EUR 108,420 as a consequence of illegally processing personal data pertaining to the formerly insured persons; the responsible individual at the second company also received a fine of EUR 20,000. These are the highest ever fines handed down by Slovenia's Information Commissioner. Further to which the Information Commissioner wishes to warn others as to its future intention to strictly impose heavy sanctions in relation to the illegal transmission or sale of personal data by the controllers of large collections of personal data.

The Information Commissioner continued its implementation of control inspection procedures instigated on the basis of its ex officio inspection procedure plan for 2009. More than one-hundred such inspections were undertaken, and among the target groups were the controllers of large personal data collections, encompassing data on employees, customers and loyalty card holders. In relation to this, companies, electronic communications operators, tourist facility providers and libraries, were inspected the length and breadth of the land, thus ensuring an appropriate level of supervision even in the remotest parts of the country.

Amendments to the Travel Documents Act and the Identity Card Act RS entered into force in 2008, and set forth conditions for the photocopying of identity cards and passports. Supervision over the photocopying of identity cards and passports had thus far been entrusted to the Information Commissioner by the legislator. In relation to this, and within the scope of ex officio inspections of controllers of personal data, the Information Commissioner also examined the legality of identity card and travel document photocopying, as well as the appropriate marking and storage thereof. It was established that identity cards and passports are all too frequently photocopied without good reason (e.g. for the purpose of ensuring the precise entry into collections, whereby simple insight and the copying of data would suffice). Data controllers were also found to have failed to obtain written consent for the taking photocopies from the holders of passports and identity cards, whilst the stored facsimiles do not contain indications which would ensure that such would not be reused for other purposes.

In 2009, the Information Commissioner continued with its pre-emptive endeavours and dedicated much attention to impact assessments in relation to privacy legislation. These activities proved particularly useful to data controllers from private and public sectors alike, especially in relation to planned amendments of legislation as well as for the preparation of projects envisaging the voluminous processing of personal data. The Information Commissioner also co-operated in several projects, pertaining to the merging of personal data collections, such as the establishment of the National Investigation Bureau and a series of projects in the field of eUprava (e-Administration) - including eZdravje (eHealthcare), eSociala (eSocial Services), eVEM (for companies), eSJU (administration) and eArhiviranje (archiving). The Information Commissioner was also engaged in public administration information security policy, as well as SRITES - the strategy for the development of information technology, electronic service provision and the merging of records.

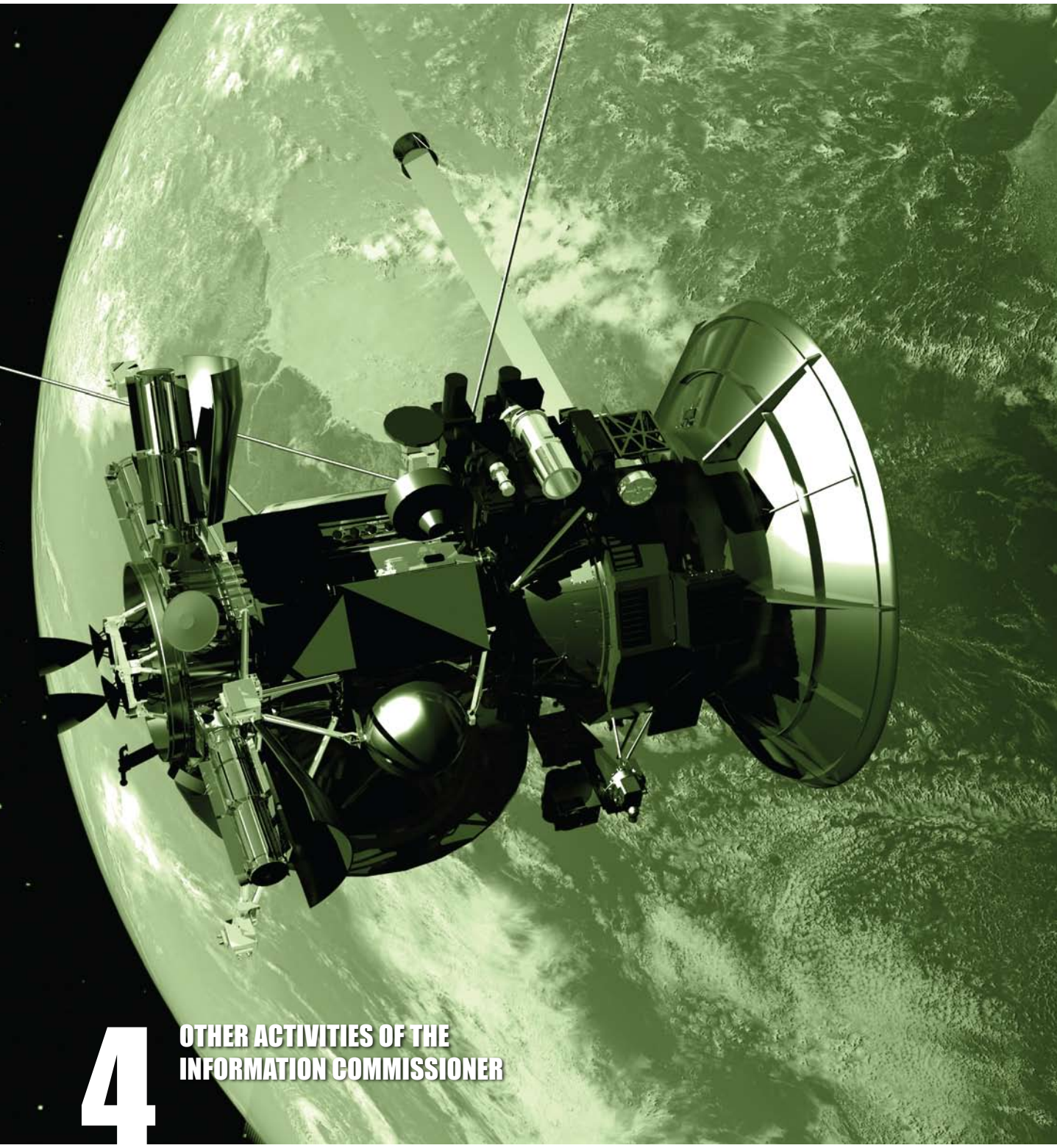
During 2009, a number of public sector data controllers and solutions providers also sought the Information Commissioner's opinion in relation to number of concepts. Of these, mention should be made of the project for informing motorists about drivers who are proceeding along the motorway in the wrong direction; the implementation of a system for the provision of behavioural advertising, targeted advertising, the recording of telephone calls, the remote signing of documents, as well as technologies for monitoring use of the Internet.

In 2009, the Information Commissioner published its profile on the popular social network Facebook, probably as first such institution, among protectors of privacy and personal data. This very popular Intrnet website has more than 300,000 users in Slovenia and over 350 milion worldwide and is primarily used for the exchange of information and personal data. Social website offer numerous useful tools, however, they can also represent a threat to one's privacy, since its users are all to often careless, in particular when it comes to publishing their own personal daza or data belonging to their friends and they often forget to set

the appropriate level of privacy, that such websites provide. The Information Commissioner's profile containes numerous publications , which pertain to the protection of personal data and the Information Commissioner will inform its 'friends' (so far over 360) on forthcoming events and significant happenings in the field of the protection of personal data, in particular in relation with the contemporary communication information technologies. The Information Commissioner will so provide another option for establishing contacts and informing on its activities.

Lastly, but by no means least, it should be pointed out that the Personal Data Protection Act has been in use, practically unchanged, since January 2005, during which time in the supervision of its implementation, the Information Commissioner has noticed several deficiencies and indeterminacies; it hence considers that it is high time that this Act was appropriately amended and corrected. It is the Information Commissioner's opinion that the definitions of terms used in this Act - in particular as regards those provisions regulating the legal basis for processing sensitive personal data; the processing of personal data for scientific and research purposes; the supply of personal data to users; protecting the personal data of deceased persons; obligations pertaining to personal data collection catalogue management; obligations in relation to the protection of personal data; deciding upon the right of an individual to familiarize themselves with their own personal data; video surveillance, and direct marketing - should be supplemented and/or amended. The Information Commissioner considers that it should obtain the right to issue fines in relation to offences, which would be higher than those currently being imposed.

The Information Commissioner is convinced that Slovenia in no way lags behind other parts of Europe as regards the various facets of personal data protection; indeed, Slovenia faces the same vexed issues, questions and problems to be found in other parts of Europe. At the same time, through the provisions of its Personal Data Protection Act, this country has established more precise and transparent regulation of certain areas of personal data protection than has been the case in the majority of European states. This holds particularly true in such fields as direct marketing, video surveillance, biometrics, the recording access (entry and exit) to premises, as well as professional supervision, and the merger of personal data collections from official records and public registers.



4 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

4.1. Participation in the Preparation of Law and Other Regulations

In compliance with the provisions of Article 48 of the Personal Data Protection Act, the Information Commissioner gives preliminary opinions to ministries, the National Assembly (parliament), self-governing local communities (municipal authorities), as well as other state institutions and bearers of public authority, as to the compliance of statutory provisions and other regulations with extant legislative regulation determining the processing of personal data. The Information Commissioner participated in the preparation of 53 acts of parliament and other legislative regulations during 2009.

4.2. Relationship with the Media

In 2009, the Information Commissioner continuously safeguarded the public character of its work and engaged in raising awareness among legal entities as well as physical persons by way of regular and consistent relationships with the media (press releases, statements, comments, interviews given by the Information Commissioner, press conferences) and through the Information Commissioner's web page. Throughout the year the Information Commissioner endeavoured to provide updated and wide-ranging web page *www.ip-rs.si*.

For the forth year in a row the Information Commissioner marked the European Personal Data Protection Day, namely by organising a special event together with the Chamber of Commerce and Industry of the Republic of Slovenia, the purpose of which was to draw attention to the importance of personal data protection, to award good practice in the field of personal data protection in private and public sector and to present awards to companies which were granted a certificate under the Information Security Management System standard (ISO/IEC 27001) in 2009 and thus demonstrated a high level of personal data protection. The central activity at the event was a panel discussion addressing the "Protection of consumers' rights and personal data processing for the purposes of direct marketing".

The Right to Know Day, which is celebrated on 28 September each year and which marks the principle of openness and transparency worldwide, saw the Information Commissioner publish on the web page a press release drawing attention to the right to be informed about all matters of general and public importance where everyone has a right to obtain information of public character without demonstrating legal interest. The objective of informed public is increasing the accountability of public sector in reaching decisions important for the public. In the Information Commissioner's view Slovenia is achieving higher standards as set forth in the Convention on Access to Official Documents in the field of access to information of public character.

The Information Commissioner provided education for liable persons and entities through its organization of a variety of workshops and seminars; further to which purpose the Information Commissioner participated in a number of conferences, workshops and panel discussions.

Among the Information Commissioner's prevention activities are the publication of guidelines which convey clear, comprehensive and useful practical instructions for controllers of personal data collections and hence provide answers to the most commonly asked questions from the field of personal data protection, which are encountered by controllers of personal data collections. By providing guidelines the controllers should gain recommendations as to how to fulfil the requirements set forth in the Personal Data protection Act in praxis. During 2009, the Information Commissioner issued the following guidelines which are accessible via the Internet:

- Guidelines for preventing identity theft,
- Guidelines for issuing court decisions for producing expert opinion,
- Guidelines for the protection of personal data in schools,
- Guidelines for the protection of personal data in media,
- Guidelines for protecting the privacy in digital television,
- Guidelines in relation with code of conduct in personal data collection,
- Guidelines Informed consumers – who do we give certain personal data and why,
- Guidelines for producing statement on personal data protection of web pages,
- Guidelines Social engineering and how to defend against it,
- Guidelines on the protection against internet harassment,
- Guidelines on the protection of personal data in integrating databases containing personal data in public administration.

Beside the aforementioned guidelines in Slovenian language, the Information Commissioner published also five guidelines in English language which are accessible via the internet:
- Guidelines regarding the introduction of biometric measures,
- Guidelines for personal data protection in employment relationships,
- Code of conduct in handling personal data collections,
- Being an informed consumer – who is allowed to handle my personal data and why,
- Media and the Protection of Personal Data.

In 2009 the Information Commissioner published its Annual Report for 2008.

In 2009 the Information Commissioner published also three pamphlets:
- How to use the Facebook and survive,
- Privacy at the workplace and
- Personal data protection in media.

A Slovene survey entitled Politbarometer conducted by the Center za Raziskavo Javnega Mnenja (Public Opinion Research Centre) at the Faculty for Social Studies, Ljubljana in its November 2009 survey looked into changing trust towards institutions and placed the Information Commissioner in the fifth place. The results revealed that 44% of respondents trust the Information Commissioner, which placed it in fifth place after the President of the Republic of Slovenia (61%), the Euro (56%), the police (47%) and the army (46%). The high level of trust in the Information Commissioner points to the fact that the public places the Information Commissioner among the most trustworthy bodies.

4.3. International Co-operation

During 2009 Information Commissioner employees took part in 16 international seminars and conferences, and they presented their own contributions at some of these events.

The Information Commissioner as a national supervisory authority for the protection of personal data co-operates with competent working bodies of the EU and the Council of Europe engaged in personal data protection. Co-operation at the international level and participation in legal procedures of the EU are envisaged also in the European Data Protection Directive (95/46/EU).

In 2009 the Information Commissioner actively participated in five working bodies of the EU, which are engaged in supervision of the implementation of various fields and facets of personal data protection across the Union, namely:
- the Working Group for the protection of personal data under Article 29 of the European Data Protection Directive (95/46/EU),
- the Joint Supervisory Body of Europol (European law enforcement),
- the Joint Supervisory Authority for Schengen,

- the Joint Supervisory Authority for customs, and
- co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national bodies for the protection of personal data (EURODAC).

In 2009 the Information Commissioner was elected a Vice-President of the Joint Supervisory Body of Europol. Whilst within the scope of police and judicial co-operation the Information Commissioner regularly participates also in meetings of the Working Party on Police and Justice (WPPJ).

The Information Commissioner also actively participated in the Internet and Information Technology Sub-Group under the auspices of Article 29 of the European Data Protection Directive Working Group, i.e. the Technology Subgroup (TS) which in 2009 engaged in online social networks, search engines, behavioural advertising and review of the EC/2002/58 Directive. The Information Commissioner actively participates also in the International Working Group on Data Protection in Telecommunications (IWGDPT), and a representative also participated in the Council of Europe's Consultative Committee for the Supervision of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (T-PD).

With the entry of the Republic of Slovenia into the Schengen zone the Information Commissioner became responsible also for the supervision of the implementation of Article 128 of the Schengen Convention and thus represents an independent body responsible for supervising the transmission of personal data for the purposes of the said Convention. In 2009 the administrator of the national part of the Schengen Information System (SIS) received 55 requests for accessing personal data in the SIS (one of the requests was filed in relation with the stolen trailer vehicle); none of the requests was rejected, while no hits were found in the SIS in 39 cases, and information on the content of the hit were conveyed to all applicants with hit in 16 cases. The period required for providing an answer to requests with no hit was 10 to 15 days, and for the requests with a hit from 26 to 60 days (depending on the promptness of the country issuing a measure). In the said period the Information Commissioner received no complaint as to the enforcement of this right at first instance. In 2009 the Information Commissioner participated in inspection group for Schengen evaluation of Romania and Bulgaria to enter the Schengen zone under the SCHEVAL.

Under the auspices of the national responsibility for supervising personal data protection in the aforementioned European databases of personal data the Information Commissioner performed inspection at the Obrežje border crossing to examine the legality of personal data processing in the SIS and an inspection on the premises of the Asylum Division as regards the implementation of the right pertaining to the asylum seekers to access information on fingerprinting for the purposes of the EURODAC and methods applied in establishing the age of juvenile asylum seekers in these procedures for the purposes of entering the data into the system.

Editor:

Nataša Pirc Musar

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
Alenka Jerše, General Secretary and Advisor to the Information Commissioner
Kristina Kotnik Šumah, Deputy Information Commissioner
Jasna Rupnik, Advisor to the Information Commissioner
Andrej Tomšič, Deputy Information Commissioner

Translation:

Ars Lingue, Tina Mušič, MA

Graphic Design:

Klemen Mišič and **Bons, d.o.o.**

Information Commissioner of the Republic of Slovenia
Vošnjakova 1
1000 Ljubljana
Republic of Slovenia

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

Ljubljana, Slovenia, June 2010

ISSN 1854-9500

REPUBLIC OF SLOVENIA