INFORMATION COMMISSIONER

'08 Annual Report Information Commissioner

2008

REPUBLIC OF SLOVENIA

'08 Annual Report

Information Commissioner

2008

0 INTRODUCTION

In 2008, we celebrated the fifth anniversary of the establishment of the Commissioner for Access to Public Information. Established in 2003 as Commissioner for Access to Public Information, the body was transformed into Information Commissioner overseeing both the right of unimpeded access to public information and the right to the protection of personal data on 31st December 2005.

The 2005 Information Commissioner Act RS enshrines and enables the equal co-existence of the right of access to information and the protection of basic human rights. Co-ordinated interpretation and a considered approach to both access and protection is exceptionally important in the recognition and maintenance of the mainstays of a democracy. An awareness as to the significance of these rights in the public domain and in everyday life amongst Slovenes increases day by day, and this in itself undoubtedly contributes towards the development of the rule of law.

In accordance with Article 14 of the Information Commissioner Act, the Information Commissioner has prepared a report as to its work during 2008, which was accordingly submitted to the National Assembly of the Republic of Slovenia. I am pleased to have established for a third successive year that the level of respect and awareness as to both the aforementioned rights continues to increase, and that this office has successfully dealt with numerous new challenges.

During 2008 the Information Commissioner handed down significantly more decisions pertaining to access to public information than it did in 2007 (82 decisions were delivered in 2007, rising to 129 in 2008). Among these cases were many complaints, the scope of which are becoming ever more voluminous and demanding. Authorities still all too frequently refer merely to the existence of a certain exemption; however, just cause, and with that the provision of hard and fast, or argued, reasons for imposition, are not evident or provided.

Last year once again witnessed a significant increase in the levy of fees for the transmission of public information, in light of which the Information Commissioner emphasizes that the cost of access to public information should remain as low as possible and, therefore, should not disproportionally impede access. It also needs to be pointed out that, according to law, labour costs may not be classified as material costs: hence our recommendation to the Ministry of Public Administration is not to approve any statement of expenditure by an authority which envisages such a possibility, e.g. the charging of an hourly rate for a civil servant who searches for certain documents or photocopies them. It is thus totally inadmissible that an applicant shall pay 300 euros for 20 pages of documents because an authority charged 30 hours labour costs for photocopying, using hourly rates applicable for an employee with university education, rather than, say, an

administrative assistant.

As regards the general impression as to the performance of authorities in the field of the access to public information, we can conclude that the initial shift in the mentality has undoubtedly been made. Good practice, already established by some, shall, in the future, have to become customary for the others.

The Information Commissioner also encounters ever more demanding and complex challenges in the realm of personal data protection and the protection of information privacy through requests for opinions and inspections. Last year the IC became engaged in some complex cases as regards personal data protection in the workplace which had been exposed by the media. A deal of attention was consequently dedicated to questions as to employee's expectations as to privacy at their workplace, particularly as regards privacy in the use of corporate electronic mail, telephones and computers, which employees also use to a certain extent for private purposes. Regarding the fact that the domain of privacy at work is under-regulated, the Information Commissioner considers that it is an area which should, in future, be more precisely defined by law.

The Information Commissioner is convinced that, in the field of personal data protection, the Republic of Slovenia in no instance lags behind other European countries; at the same time it encounters similar and very comparable problems to those which arise in all other EU states. Moreover, Slovenia's Personal Data Protection Act regulates some facets of personal data protection even more precisely and in a more transparent manner than is foreseen in Directive 95/46/EU or the legislation of most European nations. This principally holds true for such areas as direct marketing, video surveillance, biometrics, recordings of arrivals/departures from premises, linkage of personal data collections from public records and registers, as well as professional supervision.

As in previous years, the Information Commissioner has enjoyed good co-operation with all organs of the state, and thus need to resort to negative exposure has not arisen. Expert arguments, expressed in remarks to legislation and statutory procedures, contribute to improved regulatory processes and the enhanced institution of both the right of access to public information and protection of personal data. As regards legislation, the Information Commissioner continues to establish that laws which affect information privacy are often adopted too quickly, without due consideration as to their full impact or suitable risk assessment as regards the privacy of the individual. This said, however, the situation is slowly improving in this area too, and Ministries co-operate with the Information Commissioner in the preparation of legislation, especially as regards those aspects involving personal data collection and processing.

In future, pre-emptive activities should provide for the instigation and performance of preliminary privacy impact assessments, and such would be particularly important for larger projects and changes in legislation that envisages the considerable processing of personal data (e.g. the merging of ID and Health Insurance Cards). Privacy impact assessments would also be fundamental in the concept of Privacy by Design, which foresees provisions for the protection of privacy in all phases of the aforementioned projects as well as personal data processing. Privacy impact assessment is of key importance in the initial phases, due to the fact that the provision of retrospective solutions is more often than not time consuming and, at considerable cost, may also require the radical alteration of a system's concept. Thus in 2009 the Information Commissioner will issue a methodology manual for the performance of privacy impact assessments.

During 2008, the Information Commissioner dedicated considerable attention to preventive activities, hence the results of the Eurobarometer public opinion survey into public awareness, opinions and views as to the personal data protection, is really gratifying: in this survey of EU citizens, Slovenia is placed at the very top of the community's 27 member states as regards public appreciation of the problems and issues of data protection.

Over the past year the Information Commissioner issued a number of publications and guidelines pertaining to those individual areas proving to be most vexatious and problematical in praxis. Through regular ongoing contact with the media, the provision of information via its own website and, of course, through direct communication with those responsible and liable, the Information Commissioner ensured its activities were made known to all and

sundry. Its expert staff also participated in numerous informative conferences, congresses and panel discussions over the course of the year, and, during 2008, also marked 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, and all legal opinions pertaining to personal data protection and decisions pertaining to access to public information have been published in order to raise public awareness. I am also proud that our website received the 2008 Golden Netko Award for the best website in the state and public administration and associations category.

The Information Commissioner actively contributed to the development of rights at the European and international levels through its co-operation with working groups and monitoring authorities, as well as active participation in the formulation of the Convention On Access To Official Documents which was adopted by the Committee of Ministers at the Council of Europe in late November 2008.

Due to the increased scope of work, the numerous new responsibilities and enhanced international engagement, the number of Information Commissioner personnel increased last year; as of 31st December 2008, it had 30 employees.

I shall continue to strive for the work of the Information Commissioner to become ever more widely recognized and appreciated, both in Slovenia as well as abroad.

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

CONTENTS

CONTENTS

1 INFORMATION COMMISSIONER

1.1. Establishment of the Information Commissioner

On 30th 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 31st 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 1st 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.

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 question posed by a representative of the media shall be considered as a rejection deci-

1 Official Gazette of RS, No. 113/2005 – official consolidated text, 51/2007-Constitutional Court Act-A; the Information Commissioner Act (ZinfP).

2 Official Gazette of the Republic of Slovenia, No. 110/2006, official consolidated text; Public Media Act (ZMed).

sion. 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 Act on the Access to Information of Public Character (ZDIJZ)[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 Act on the Access to Information of Public Character with regards to the appeal procedure, the provision of article 45 of the Public Media Act and the Personal Data Protection Act (ZVOP-1)[4].

Pursuant to the second paragraph of Article 112 of the Electronic Communications Act (ZEKom)[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 (ZPacP)[6], the Travel Documents Act (ZPL)[7] and the Identity Card Act (ZOIzk)[8].

The competences of the Information Commissioner arising from the Patients Rights Act - ZPacP - 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

3 Official Gazette of the Republic of Slovenia, No. 51/2006, official consolidated text and 117/2006-ZDavP2; Act on the Access to Information of Public Character (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 - Electronic Communications Act (ZEKom).
6 Official Gazette of RS, No. 15/2008; ZPacP.
7 Official Gazette of RS, No. 3/2006 – official consolidated text, and 44/2008; ZPLD.
8 Official Gazette of RS, No. 71/2008 – official consolidated text; ZOIzk.

from medical documentation (seventh paragraph of Article 45 of the ZPacP).

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

- 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 - ZPL:

- 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.

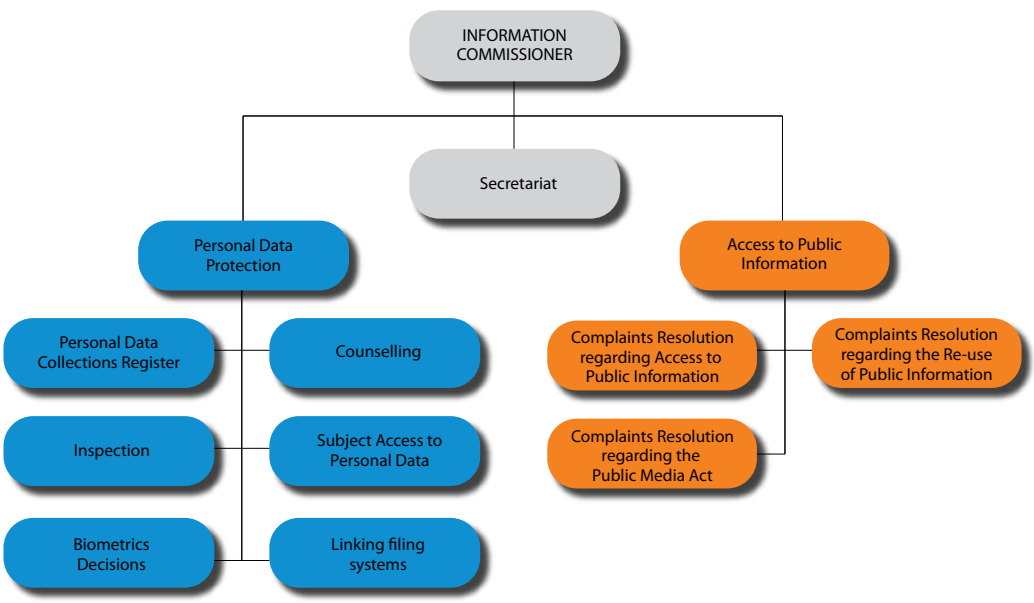
1.3. Organization of the Information Commissioner

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

Diagram 1: Organization



Due to the increased scope of work, as well as due to several new fields of jurisdiction and international engagements, the number of employees increased in 2008. On 1st January 2008 the Information Commissioner had 29 personnel; this number had risen to 32 by year's end (two of them employed on temporary basis). All those working as civil servants within the organisation have university degrees.

1.4. Finances

The work of Information Commissioner is financed from the state budget; funding is apportioned by the National Assembly of the Republic of Slovenia (parliament) on the basis of a proposal by the Information Commissioner (see Article 5 of the Information Commissioner Act). At the beginning of 2008, this allocation amounted to 1.282.859,00 euros, rising to 1.299.644,09 euros at year's end. During fiscal 2008, the Information Commissioner had spent 1,237,544 euros, namely:

- *943.148,00 euros for salaries and other employee expenses;*
- *323.629,00 euros in material costs;*
- *21.703,00 euros in investments and capital expenditure.*

Accordingly, 99.39 % of the available budget for 2008 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[9]. 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[10]. 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 during 2008

169 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 2008. The Information Commissioner issued 129 decisions, 9 cases were carried over from 2007. The number of decisions in the field of access to public information has significantly increased compared to 2007.

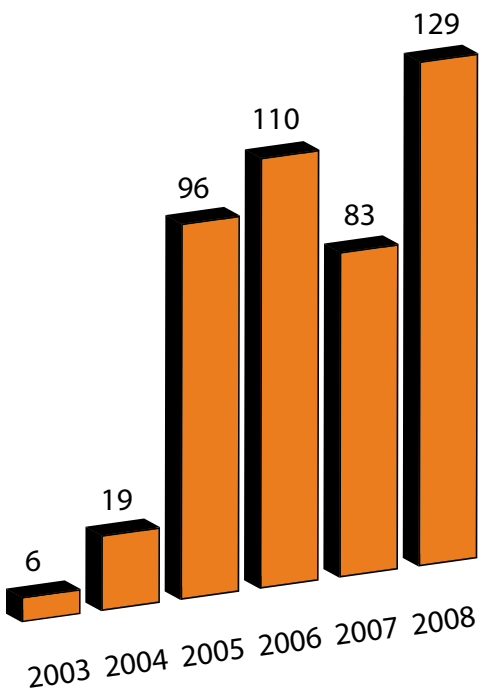


Diagram 2: Number of decisions handed down in relation to access to public information, 2003-2008.

9 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.

10 Official Gazette of the Republic of Slovenia, No. 24/2003; Act on the Access to Information of Public Character (ZDIJZ).

As regards the decisions the Information Commissioner:

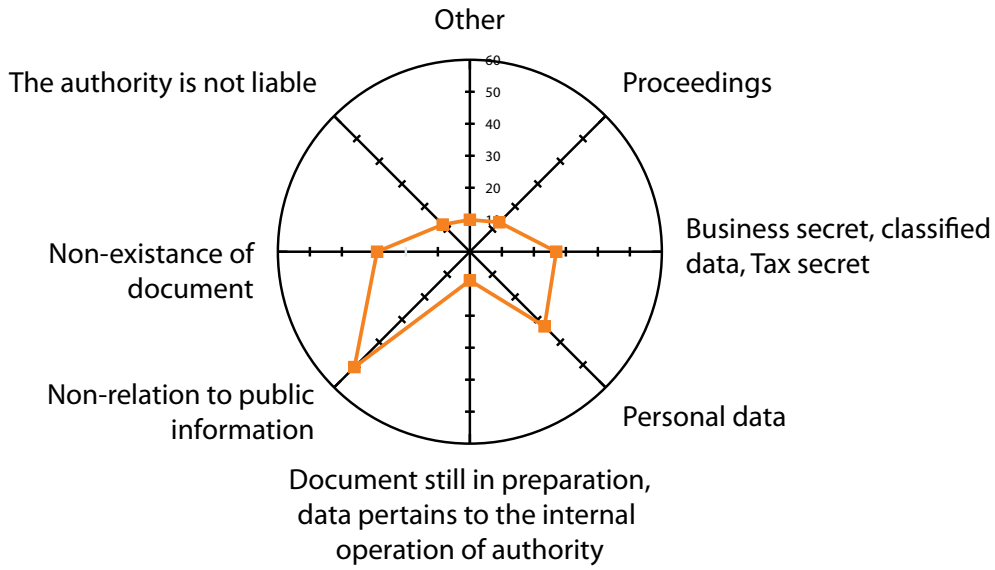
- resolved the matter in favour of the applicants in 32 cases
- rejected the complaints in 47 cases
- partially approved access in 37 cases, and
- returned the matter to the first instance authority in 10 cases
- in two cases the Information Commissioner rejected the complaint as inadmissible, and in one case the decision of the first instance authority was declared void.

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

- whether the requested document fulfilled the conditions for the existence of public information in accordance with the 1st paragraph of Article 4 of the Act on the Access to Information of Public Character (51);
- whether the requested document included personal data, the disclosure of which would contravene the provisions of the Personal Data Protection Act (33);
- whether the applicant requested information and/or data considered a business secret, according to the act regulating companies (22);
- whether the liable person or authority holds the document or the public information which has been requested by the applicant (29);
- whether the authority, to which the request for public information was addressed, is liable to provide information in accordance with the Act on the Access to Information of Public Character (12);
- 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 which was obtained or compiled consequent to a civil procedure, or a non-litigious civil procedure, or some other legal procedure, and disclosure would harm the execution thereof (5);
- 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 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 (5);
- whether the requested information is data which was acquired or put together consequent to an administrative procedure, the implementation of which would be harmed by premature disclosure (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 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 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 (4).
- 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 (3);
- whether this is an instance of the re-use of public information (3).

In 2008 the Information Commissioner issued six 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.

Diagram 3: Decisions taken in relation to the Act on the Access to Information of Public Character 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 (57);
- Public funds, institutes, agencies and other entities subject to public law (25);
- Administrative units and municipalities (18);
- Courts and the State Prosecutor's Office (14);
- Educational institutions (9);
- Health authorities (1);
- Ombudsman of the Republic of Slovenia (1).

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

59 applications were lodged by private individuals, in 17 instances the applicants were journalists and on 23 occasions NGOs, various associations and societies. In 20 instances private sector legal entities, lodged complaints as to the lack of provision of requested information; the Information Commissioner also received two complaints by municipalities and one by a public sector legal entity.

In 2008, 18 lawsuits were filed at the Administrative Court against decisions made by the Information Commissioner, a figure which represents 14% 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 2008, the Administrative Court RS had rendered 28 judgements in lawsuits against the decisions made by the Information Commissioner. In 22 instances the contested decision was annulled and the matter returned to the Information Commissioner for reconsideration; in 1 case the suit was partially granted, and in 4 cases the Administrative Court rejected the complaints.

In 2008 the Supreme Court decided upon 2 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 2008, the Information Commissioner received 259 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 221 cases the liable body granted an applicant access to the requested information.

102 requests for help and various questions posed by individuals were addressed to the Information Commissioner during the course of 2008, 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 2008 one proceeding was initiated for each: infrigments due to the violation of Article 23 of the Access to Public Information Act; Article 45 of the Mass Media Act and Article 10 of the Information Commissioner Act. A warning was issued for the perpetrator of the violation of Article 23 of the Access to Public Information Act and the proceedings against the perpetrators of the violation of provisions of the Mass Media Act and the Information Commissioner Act were suspended.

2.3. Some Significant Case Law

By way of its Decision No. 021-61/2008 of 6th November 2008, the Information Commissioner rejected an appeal by Amnesty International Slovenia against the Police Service RS. The applicant requested data on the number of so-called 'erased persons' who were - or still are - in the process of being deported from the country; the number of 'erased persons' who have actually been deported from Slovenia and a description of possible guidelines or instructions provided by the Ministry of the Interior or the Police Service to serving police officers and/or to the so-called Aliens Centre as regards the implementation of the Aliens Act RS (Zakon o Tujcih)[11] in relation to 'erased persons'. The applicant then subsequently requested data on the formal state of the procedure for the deportation of aliens from the country. Having considered all the stated facts, the Information Commissioner decided that no legal grounds existed for the Police Service to merge data filing systems governed by the Aliens Act RS, with the central population register to thus obtain the information requested by the applicant. Such processing of personal data would also be in conflict with the provisions of the Personal Data Protection Act (ZVOP-1). Notwithstanding the fact that the applicant requires merely the number of individuals described as so-called 'erased persons', who have been subject to the deportation procedure, such information would still only be obtainable by processing personal data. The criteria of an extant material form - a prerequisite for public information being deemed to exist - was not fulfilled in this instance, because the Police Service does not dispose of the data requested by the applicant. The body in question is not obliged to collect such information from others, nor is it obliged to process or analyse such, as was requested by the applicant, and hence create a new document consisting of unprocessed, dispersed data and in such way enable any immediate familiarization with the requested information.

By way of its Decision No. 021-124/2008/12 of 19th December 2008, the Information Commissioner partially granted the appeal of an applicant against the Medvode Munici-

11 ZTuj - Official Gazette of the Republic of Slovenia, No. 1/1991; and ZTuj-1 - Official Gazette of the Republic of Slovenia, No. 71/2008 – consolidated text.

pality (Občina Medvode), annulled the contested decision made by Medvode Municipality and ordered that the authority should provide the applicant, within 15 days upon receipt of the Decision, photocopies of the requested documents in relation to travel, paid for by the municipality, and at the same time also to redact certain personal data pertaining to persons who are not civil servants, and which, as such, represents protected personal data. The requested information is per se related to the activities of the public authority since it pertains to appropriation by that authority. The Information Commissioner emphasized that the potential negative estimation which the applicant or the general public might gain - either justifiably or unjustifiably - following the disclosure of a certain information, pursuant to the Access to Public Information Act, is not a valid argument for preventing access to the information. Information which may reflect badly on the liable public authority - e.g. inappropriate action, poor management, tardiness, non-responsiveness, and even corrupt or unethical practices which may well prove to be a criminal offence - are frequently in the public interest, and hence access to such information is assessed as being 'in the prevailing interest of the general public'. The supervisory function enables citizens to oversee the work and financial appropriation of public administration and authorities, for the very reason it prevents bad management, the abuse of power and corruption.

By way of its Decision No. 021-75/2008/7 of 17th December 2008, the Information Commissioner upheld the complaint of Inter Koop d.o.o. against Slovenia's Ministry of Defence (hereinafter MORS). The applicant stated that it had requested access to the tender documentation of all bidders in a public tender for the provision of cleaning and sanitary materials - MORS 51/2007, and specifically: to the annexes of all 8 applicants for all sections (re suitability of tendered products of individual bidders). The Information Commissioner decided in favour of the applicant and requested that MORS enable the access to the requested documentation within 15 days of receipt of the Decision. Pursuant to the Public Procurement Act[12], MORS, as the administrative authority, is obliged to implement the provisions of the said Act, when carrying procurement. Public procurement procedures must be transparent and this also extends to any request for disclosure. Transparency and publicity of procurement procedures are defined as being in the public interest as well as in the interest of individual bidders, whereas the purpose and the manner of public procurement must be evident. Consequent to the principle of transparency, the Public Procurement Act (ZJN-2) explicitly provides that certain documents are of a public nature, and hence their exemption as a "business secret" is inadmissible. The price stated in a bid can never be regarded as a business secret and neither can - when pondering the criteria of the most favourable bid - that data which reflects the fulfilment of terms and conditions. Through access to public information, the general public namely must be able to check whether the selected bidder has satisfied all the conditions and criteria set forth in the published tender. By way of such practice the supervisory function, namely the right of public access to public information, can be exercised, and such practice helps prevent mistakes made in public procurement procedures, as well as bad management, together with inadequacies, failures and abuses in the exercise of power and authority as well as the administration of public funds. Every person who enters into a business relationship with a state or public authority and/or wants to win a public tender must be aware that their freedom in defining the data they provide as a business secret is limited due to the very reason of transparency, particularly so when such data relates to use of public funds. All parties must be aware that they cannot expect to enjoy complete business secrecy in relation to contracts signed on the basis of public tenders.

By way of its Decision No. 021-47/2008 of 22nd April 2008, the Information Commissioner upheld an application in relation to the Domžale District Court (Okrajno Sodišče v Domžalah) to mail photocopies of requested information to the applicant. The applicant requested a document from which it was evident when the Court had received the payment for the full purchase price for a certain piece of real estate which was sold at public auction, as well as when, in what manner and to which account the Court transferred the money to the creditor. The Information Commissioner established that exercising uni-

12 Official Gazette of the Republic of Slovenia No. 128/2006.

versal jurisdiction (which includes permission for execution of judgements and insurance of claims) is a part of the tasks of public authorities and hence belongs to their scope of work. The requested documentation pertains to an enforcement procedure (in accordance with Article 5 of the Execution of Judgments in Civil Matters and Insurance of Claims Act) under the jurisdiction of a district court, in this instance the Domžale District Court. The Information Commissioner has established that the date of the receipt of the funds, namely the purchase price of the designated real estate, is in fact public information. The Court is hence obliged to provide the applicant with documents in relation to the receipt of the remunerated funds and the statement concerning payments, from which the day of the payment is evident. Information in relation to the creditor and the number of his bank account, which in this case arises from the decree in relation to the execution of the judgement, does not represent a tax secrecy exemption. However, since such documentation also includes other data, not requested by the applicant, it must be accordingly redacted by the authority (Court).

By way of its Decision No. 021-141/2008 of 18th December 2008, the Information Commissioner decided that the complaint of an applicant against the Municipality of Ljubljana was well-founded and that the municipal authorities must provide a photocopy of the requested document within five days, or enable access to the independent assessment consisting of two documents, namely: Assessment of the Strategic Spatial Plan and Draft Assessment of the Implementation Plan (hereinafter: the assessment) made by the Dutch urban planner Jan Vogelij, in relation to the new generation of planning statutes implemented by the Municipality of Ljubljana. Said applicant was interested in the neutral, politically unburdened opinion of the Dutch planning consultant in relation to Slovenian spatial planning. The applicant accordingly requested from the authority a document in which the independent expert produced an assessment of the spatial planning acts adopted by the Municipality of Ljubljana. The assessment had been commissioned by the authority, which had also stated that a contract had been signed with the independent expert assessor for this purpose. The Information Commissioner established that in this particular instance none of the three elements which are a pre-condition for the existence of an exemption pursuant to point 9 of the first paragraph of Article 6 of the Access to Public Information Act were present, since the assessment had been made by an independent foreign expert who was no longer in the process of drafting the assessment; indeed, said assessment had been completed and submitted to the authority. The Information Commissioner further pointed out that one should not ignore the fact that the authority had ordered the requested document from an outsourcer and paid for the service from the budget of the Municipality of Ljubljana, which means that in this instance it should be regarded as public information since it had been paid for using funds from the public purse. In the event that public funds have been used, the Access to Public Information Act expressly emphasizes the need for the transparency of the operations of authorities, and the significance of public oversight as to the rectitude of operations in the public sector.

By way of its Decision 0900-243/2008 of 10th December 2008, the Information Commissioner rejected an appeal by an applicant against the parliamentary party of the Slovenian Democratic Party (SDS). The applicant filed a request addressed to the SDS, in fact to the leader of its parliamentary party, for access to allegedly public information, whereby the transcript of an audio recording was requested. Said transcription derived from clandestine recordings of the Croatian Prime Minister, Mr. Ivo Sanader, made between 1st January and 1st December 2004 by Slovenia's National Intelligence and Security Agency. The Information Commissioner established that neither the SDS nor the leader of its parliamentary party were liable for the provision of such information, and furthermore neither the SDS or its parliamentary party independently or together carry out a public service or the function as a public authority, but are instead - as regards the parliamentary party - a forum under which members of parliament are organized in order to more easily exercise their rights and obligations within the scope of their work in the National Assembly. The leader of the parliamentary party is a member of Parliament, who represents the parliamentary party; pursuant to the provisions of the Access to Public Information Act, such a person and functionary is not a body within the meaning of the first paragraph of article 1 of the

Access to Public Information Act. Indeed, in this instance the body is National Assembly of the Republic of Slovenia - parliament - within the scope of which individual parliamentary parties, which also appoint their various leaders, are organized.

2.4. Overall Assessment and Recommendations re Access to Public Information

The right of access to public information is deemed a basic human right, as identified under the second paragraph of Article 39 of the Constitution of the Republic of Slovenia. The purpose of the Access to Public Information Act RS, which arises from the fundamental principle of transparency, reflects the democratic, economic and supervisory functions of the right of access to public information. The Information Commissioner emphasizes that the principle of openness exercised by public authorities cannot merely be limited to the various forms of parliamentary decision-making but should also embrace all forms of direct co-operation with citizens in the adoption of political decisions and the laying down of statutory provisions. The institution of access to public information enables the citizen to become acquainted with the content of activities performed by public authorities and to actively participate in their implementation. The supervisory function enables the citizen to oversee the work of public authorities and administration, whereby rectitude is ensured, and mismanagement, abuse of power and corruption prevented. By means of communication and the development of a closer and more open relationship between the individual citizen and organizations and authorities operating in the public sector, trust in the administration shall be enhanced through better understanding. Consequently the public at large shall no longer perceive the operations of public authorities as imposition, but rather the acceptable institution of democracy. The Information Commissioner - as a public sector authority acting in appeal procedures as well as in the exercise of its competencies in relation to access to public information - likewise operates in this same spirit of openness and transparency.

Based on the general impression as to the response of liable authorities with regard to access to public information, it can be perceived that an initial shift in the basic mentality has occurred, and that a number have already established quality modi operandi in this area. Although 2008 witnessed a significant increase in the number of appeals re issues relating to the Access to Public Information Act - the number of decisions issued by the Information Commissioner rose from 82 in 2007, to 129 in 2008 - it can at the same time be ascertained that the appellate cases have become more extensive and demanding as regards their content. In several cases the Information Commissioner annulled the first instance decision issued by a liable authority because it had established that procedural rules had been significantly violated and/or that where was insufficient evidence to support the pronouncement of the decision. All too frequently liable authorities merely referred to the existence of a certain exemption; however, any actual substantiation as to the nature or reason for such was not evident from the explanation behind the decision.

Based on actual appeal procedures, the Information Commissioner assesses that 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 becoming aware that the more freely accessible information they publish on their websites, the fewer formal requests they are likely to receive from applicants. Consequently, upon their own initiative and volition, they are publishing significantly more public information on their websites, without any resort to requests by applicants. The Information Commissioner assesses that authorities are increasingly employing the provision of the fifth paragraph of Article 6 of the Access to Public Information Act, which maintains that if said information is available from freely accessible public registers or is in another way publicly accessible (publication in an issues of the Official Gazette RS, other publications, media, the Internet and such-

like), the authority may instead provide instructions as to the location of the information, rather than elect to provide the applicant with the requisite information. At the same time, however, all too many authorities subject to the Access to Public Information Act perceive this legislation as something which solely imposes an obligation to deal with applicants, and that having to enable public access to public information diverts them from their basic tasks and operations. It should be added that such a perception of legal obligation is characteristic, in particular, of those parts of the public sector which are not organs of the state or public administration in its narrower sense, such as lesser public authorities, public institutions, legal entities and public service providers (particularly at the local and municipal level). These organizations frequently ascribe their diminished attention and care for freedom of access to public information to such burdens as their mandatory operational workload, insufficient human resources, even insufficient budgetary resources and - most of all - to insufficient familiarity with the Access to Public Information Act. All of the above excuses are all too often used as justification for their silence.

The Information Commissioner has observed that the requisite information was forthcoming during many appeal procedures instigated as a consequence of a lack of response or reply by the liable authority; it is arguably apparent that said authorities need more time than the twenty working days foreseen 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 the 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. 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 the decision in the appeal procedure.

The Information Commissioner has perceived a significant increase of cases in which the liable authority does not dispose of the requested information, and hence the so-called materialized form criteria, as a prerequisite for deeming the existence of public information was not fulfilled. In the opinion of the Information Commissioner, the above is also a consequence of the fact that the liable authority has insufficient respect for the principle of provision of legal assistance to the unknowing applicant beyond the scope of the procedure which regulates access to public information. It has also been noticed that some applicants, who are aware of their right to appeal in their quest for access to information pursuant to the Access to Public Information Act, actually wish to expose other deficiencies pertaining to the work of liable authorities, which are not in direct correlation with access to public information.

The Information Commissioner has dealt with several cases in which applicants were aware that the authority did not dispose of the requested public information; however, they had lodged an appeal in order to warn as to the non-existence of certain information which, taking into consideration substantive regulations, should have existed. Such obligations arise not from the Access to Public Information Act but rather from other statute regulating their field of work. Pursuant to the provisions of the first paragraph of Article 1, as well as the first paragraph Article 4 of the Access to Public Information Act, public information shall be deemed to be that which the authority has acquired from other persons or emanates from its field of work or operations, and occurs in the form of a document, drawn up by that body. Pursuant to the Access to Public Information Act, liable authorities are only obliged to provide access to extant information, and are not obliged to acquire additional information or create a new document which was not in existence at the time when the applicant lodged the request. The Information Commissioner hereby emphasizes that in the procedure pertaining to access to public information, it is has no competence as regards any assessment as to the legality and expediency of the operations of liable authorities, nor the question as to why authorities do not dispose of documents they should dispose

of; nonetheless, it should also be emphasized that liable authorities are failing to operate appropriately or transparently in those cases when they do not act in compliance with their legitimate competencies. Such a notion is particularly germane in instances where applicants are not provided access to public information due to the inactivity of a liable authority which avoids, by means of omission of due activities, its obligations under the Access to Public Information Act.

It has yet again been noted that liable authorities are not aware of the explicit legislative provision which states that applicants do not need to invoke the Access to Public Information Act when requesting access to information, and that liable authorities are obliged to consider the matter in accordance with said Act, whenever it is perceivable from the nature of the request itself that this is a request in accordance with the Access to Public Information Act. As a consequence, requests for access to public information are all too often considered as requests for a review and transcription of files in accordance with procedural regulation which demands a legal interest or reasonable benefit to be exhibited. As a consequence, liable authorities often erroneously demand that applicants should supplement their requests for access to public information, or even wholly reject such requests because legal interest had not been shown. This is not consistent with the basic tenet of the Access to Public Information Act which maintains that no legal interest is necessary for access to public information, and that public information is freely accessible. Each applicant shall, upon any request, have the right to acquire information from the authority, in person, on the spot, or through the provision of a transcript, photocopy or an electronic record of such information.

The Information Commissioner has observed that there have been numerous cases in which a liable authority has been overly formal in its handling of requests - by, for example, demanding that a request be supplemented. As a consequence the authority was able to dismiss an applicant's request without any consideration as to its content. Here it should be stressed that the procedure surrounding access to public information is an informal one, and hence communication between an applicant and the liable authority should be carried out in a spirit of openness and freedom of access to public information, rather than with the aim of impeding access to such information. Applicants commonly request extensive documentation, often this is merely due to the lack of knowledge with regard to information available from the liable authority, and thereby an extensive request for access is unduly created. In accordance with the principle of assistance, liable authorities should support an unknowing applicant by searching for the type of public information that the said applicant is interested in. Even when an applicant requests vast and all-encompassing information, the liable body should not reject access merely because of the possibility of the additional work that will be necessary in searching for and preparing the documentation in question.

A significant increase in the charges levied for the provision of public information was yet again perceived during 2008. In the light thereof the Information Commissioner emphasizes that the charges for access to public information shall be kept to a minimum, and specifically such levies should not disproportionally impede access. According to the Access to Public Information Act, access to requested information shall be provided free of charge, while the *Decree on Communication and Re-use of Public Information*[13], governing provision, seems to represent a problem since it allows an interpretation whereby a liable authority may determine the cost of services that it provides in relation to the facilitation of access. By way of such methodology, consent has been provided for a tariff which enables an authority to charge for information searches, the examination of information, its preparation for partial access, as well as photocopying or retrieval from an information system. In a number of cases examined by the Information Commissioner, authorities have abused this provision and implemented tariff regimes which have levied unjustifiable charges for the services provided; by way of this practice, liable authorities have repeatedly impeded access to information, and thus the exercise of this particular human right. In light of this, the Information Commissioner emphasizes that the tasks of liable authorities pertaining to their meeting the provisions of the Access to Public Information Act, are those

13 Official Gazette of the Republic of Slovenia, No.. 76/2005, with amendments and supplements.

which relate to the execution of public services and thus the fulfilment of their mandate; they are not services provided on the market, for which they are entitled to charge freely.

In relation to - and as a consequence of - all the issues stated above, the Information Commissioner warns that non-critical and disproportionate levies of charges for the provision of information brings the entire system of access to public information into question, and in principle it opposes the application of tariffs which enable the levy of arbitrary or uncontrolled fees. Due to inappropriate regulation of this issue, the Information Commissioner also assesses that in this particular area, costings and charges should also be regulated differently in the *Decree on Communication and Re-use of Public Information*.

Last year the Information Commissioner yet again noted a decrease in appeal procedures in relation to the re-use of public sector information, the underlying reasons for which could be inactivity or a lack of applicant interest. 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 (duty) for which the documents were 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.

The primary aim of re-using or taking advantage of public information is for the applicant to upgrade the value of such information, and thereby perform an economic function through the right of access. Realizing such commercial functions 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 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[14] was adopted by the National Assembly of the Republic of Slovenia on 15th July 2004, and has been in force since 1st 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[15].

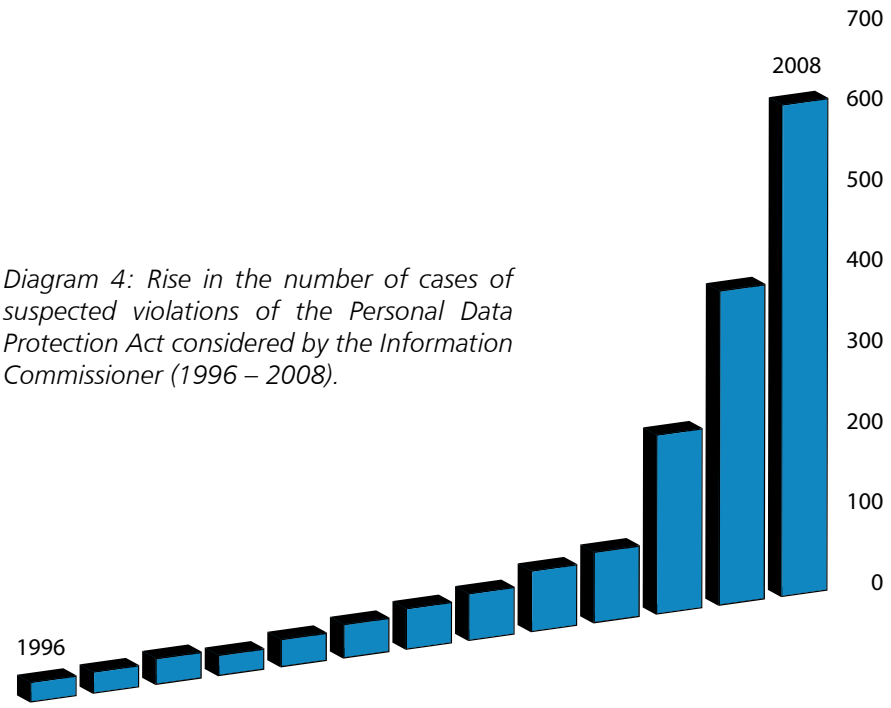
In July 2007, amendments to the Personal Data Protection Act (ZVOP-1) were adopted by way of the Act Amending the Personal Data Protection Act[16]. This legislation (ZVOP-1A) introduced two important novelties, namely from the perspective of the administrative and - as a consequence thereof - the financial 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 (ZVOP-1-UPB1) has been published in September 2007. The provisions of the Personal Data Protection Act-1A (ZVOP-1A) were harmonized with the amendments to the 2006 General Offences Act[17], and also took into consideration the introduction of the Euro, which was adopted as the national currency in Slovenia on 1st January 2007.

14 Official Gazette of RS No. 86/2004 - Personal Data Protection Act (ZVOP-1).
15 Official Journal of the European Union, No. L 281, 23rd November 1995.
16 Official Gazette of RS, No. 67/2007; Personal Data Protection Act - amendments (ZVOP-1A).
17 Official Gazette of RS No. 3/2007 - official consolidated text, General Offences Act (ZP-1).

3.2. Review of Activities in the Field of Personal Data Protection in 2008

During 2008, the Information Commissioner received 635 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act (ZVOP-1); namely 256 in the public sector and 379 in the private sector. There were 192 applications and complaints against public sector legal entities, 64 procedures were initiated ex officio, whereas 310 applications and complaints were made against private sector entities, and 69 procedures initiated ex officio. Statistical data indicates that the number of applications as to alleged violations of the Personal Data Protection Act (ZVOP-1) continues to rapidly increase year on year. Following assessment of the received applications and ex officio cases, 216 inspection procedures were initiated in relation to public sector entities and 316 in private sector entities. On the basis of Article 33 of the Inspection Act[18], 55 cautions were issued in relation to minor irregularities. 61 regulatory and administrative decisions were also handed down, whereby the liable persons were ordered to undertake measures to rectify the established irregularities. 348 inspection procedures were concluded with a decision to stay the proceedings.

Diagram 4: Rise in the number of cases of suspected violations of the Personal Data Protection Act considered by the Information Commissioner (1996 – 2008).



In 2008, most cases of suspected violations of the Personal Data Protection Act pertained to:

- illegal collection or request for personal data (183 instances);
- disclosure of personal data to unauthorized users by a personal data collection controller (117);
- illegal publication of personal data, for example on notice boards and in the media (63);
- illegal video surveillance (46);
- insufficient security measures to ensure adequate prootection of personal data (31);
- misuse of personal data for the purpose of direct marketing (29),
- 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.

18 Official Gazette of RS, No. 43/2007 - official consolidated text; Inspection Act (ZIN).

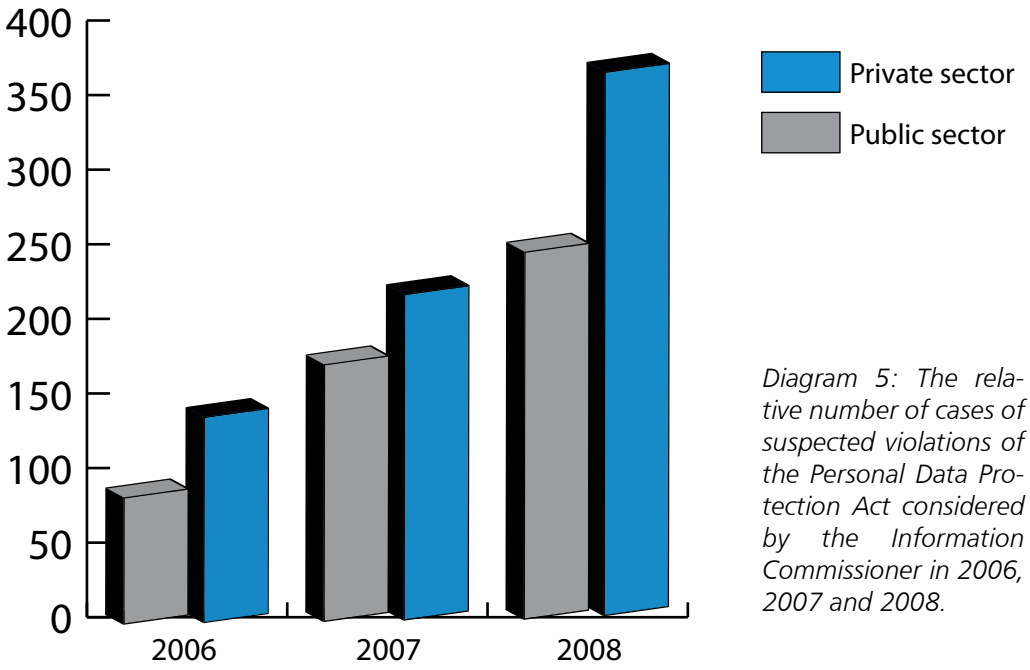
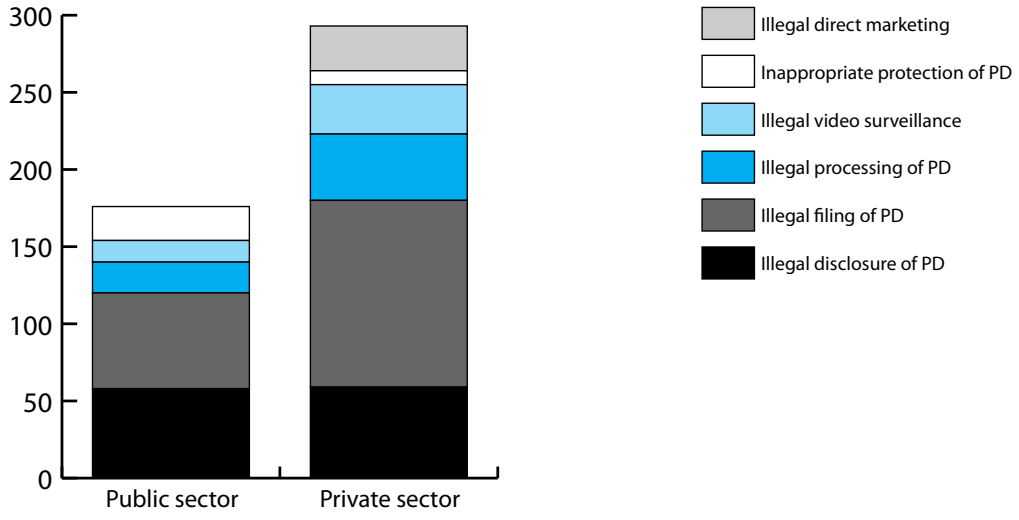


Diagram 5: The relative number of cases of suspected violations of the Personal Data Protection Act considered by the Information Commissioner in 2006, 2007 and 2008.

Diagram 6: The illegal processing of personal data in 2008 as identified by the Information Commissioner; a comparison of the public and private sectors



The established violations and irregularities in the field of personal data protection were mostly the same, or very similar, to those recorded in previous years. In the majority of cases, irregularities in personal data protection emanated not as a consequence of deliberate violations of the Personal Data Protection Act but - above all - as a consequence of the data controllers' lack of familiarity with the provisions of said Act, or a mere lack of attention as regards the protection of personal data.

279 violation procedures were initiated in 2008 as a consequence of violations of the provisions of the Personal Data Protection Act (ZVOP-1); these were namely: 49 procedures against public sector entities, 78 against legal entities in private sector, and 155 procedures against individual persons. The violation proceeding is entertained in accordance with the Personal Data Protection Act (ZVOP-1). As a consequence of established violations, the Information Commissioner issued:

- 40 warnings (three in proceedings initiated in 2007),

- 131 decisions regarding violations (encompassing 103 cautions, eight thereof in relation to proceedings initiated in 2007, and 28 fines, three of which pertained to proceedings initiated in 2007),
- 3 payment orders.

In 2008, 19 offenders lodged applications for judicial protection; ten against fines, and nine against cautions.

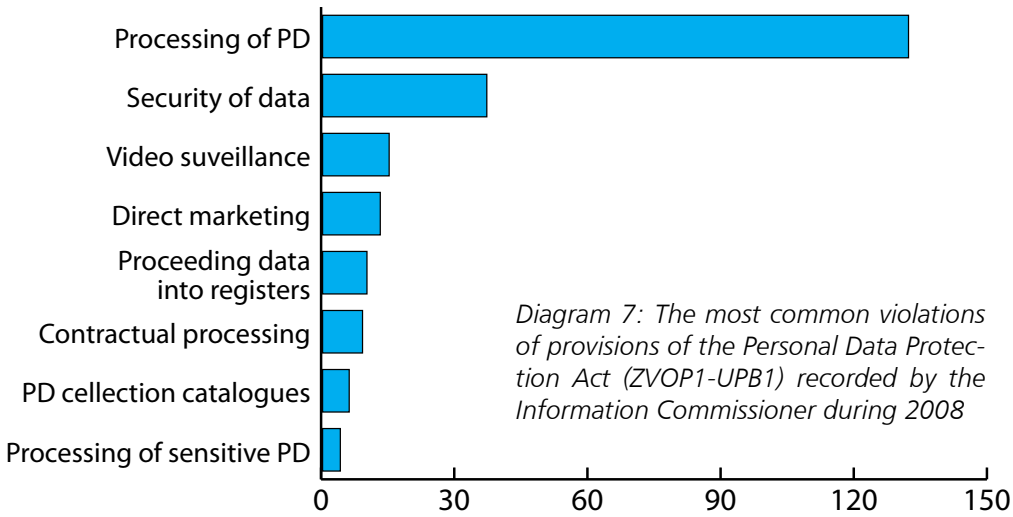


Diagram 7: The most common violations of provisions of the Personal Data Protection Act (ZVOP1-UPB1) recorded by the Information Commissioner during 2008

In 2008 the Information Commissioner received 853 requests for written clarifications or opinions regarding specific issues, which is fewer than in 2007, when the Information Commissioner received 1144 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 also provided oral opinions and clarifications. An IC employee is on-duty from 8 a.m. to 4 p.m. every day to answer telephone enquiries.

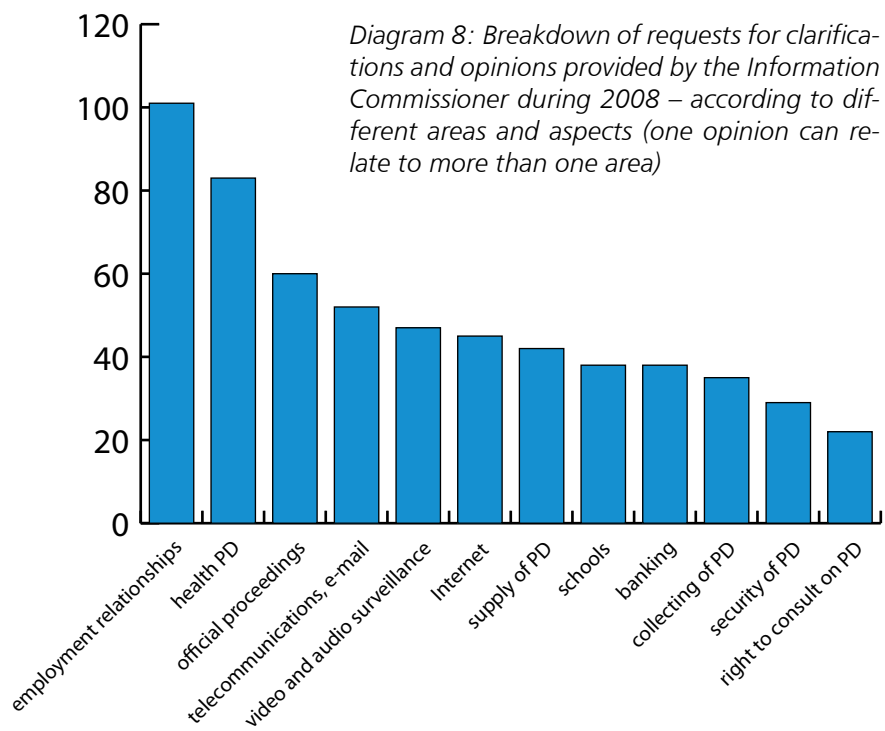


Diagram 8: Breakdown of requests for clarifications and opinions provided by the Information Commissioner during 2008 – according to different areas and aspects (one opinion can relate to more than one area)

The Information Commissioner received 40 applications concerning the implementation of biometric measures during 2007, whereas in 2008 it received 16 applications, twelve from private sector legal entities, and four from public sector operators. Fifteen decisions as to the admissibility of biometric measures were issued in 2008, of which two were applications lodged in 2007; ten decisions vindicated the implementation of biometric measures, limited implementation was approved in three instances, while two decisions proscribed the introduction of biometric measures.

In relation to the introduction of biometrics, the Information Commissioner assesses the applicant's objective, which must be justifiable and substantiated by sufficient proofs. It also establishes whether the same purpose could be achieved with other methods of verification or establishing identity that would not encompass biometric measures, and are hence less invasive as regards the privacy and dignity of employees. The Information Commissioner also assesses the technical aspects of biometric measures in establishing, ascertaining and authenticating identity.

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 permitted the implementation of biometric fingerprint identification for employees entering premises housing sensitive telecommunications equipment, as well as special software and servers, encompassing business secrets and other particularly sensitive data. 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 2008, the Information Commissioner received eight applications for the export of personal data. It issued six decisions, one of them in relation to an application received in 2007. All applicants who received decisions were allowed to export the data. These were as follows:

- for the purpose of the management of online savings accounts, the subsidiary of a foreign bank operating in Slovenia was permitted to export data in relation to the personal identification of its clients to a data operator subcontractor in India;
- the Slovene subsidiary of a foreign enterprise was allowed to export and transfer personal data pertaining to its employees to a data operator in the USA in relation to the solution of complaints pertaining to subcontractor employment relationship;
- a telecommunications operator was authorized to export and transfer personal data in relation to its subscribers and pre-pay users, as well as users of its on-line services, to a Croatian data operator subcontractor;
- a telecommunications operator was allowed to export and transfer personal data pertaining to its employees and their dependents to a Croatian data operator subcontractor, for the purpose of the development, implementation and maintenance of human resources software;
- a trading company was permitted to export and transfer the personal data of bonus card holders to its Vietnamese subcontractor for the purpose of issuing cards to its clients;
- an educational institution was authorized to export and transfer the personal data of its students to a data operator subcontractor in the USA, for the purposes of creating digital identity in the form of a username and a password which enables access to an e-student web portal as well as other information services.

The Information Commissioner received 12 applications for permission to merge personal data during 2008. Eight positive decisions - three of which were issued in relation to applications lodged in 2007 - pertained to the granting of permission for the merging of one

data filing systems with one or more other data collections. These decisions encompassed such issues as the merging of a data collection on foreigners with the record of insured persons with compulsory medical insurance, the Record of legal enforcements with the tax register; basic medical documentation with the central population register (EMŠO), and likewise the register of births marriages and deaths; the insolvency register with the central population register (EMŠO). 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 filing systems are only permissible as regards certain types of personal data determined by law.

During 2008, the Information Commissioner received 48 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 various Ministry of Health bodies and the failure to disclose personal data which pertained to the applicant. 33 of the received applications were addressed, including one application from 2007. In fifteen instances the data controllers disclosed the data immediately upon receiving a call from the Information Commissioner, in four instances data controllers were obliged by the decision of the Information Commissioner to allow the applicant access to their own personal data; three applicants were referred to the competent institution and/or the data controller, three applicants withdrew their complaints, and nine 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 2008, the Information Commissioner lodged two applications for constitutional review:

Request for assessment as to the constitutionality and legality of the third and fourth paragraphs of Article 390 of the Banking Act[19]*:*

The contested provision of the aforementioned law is insufficient to satisfy the constitutional request for an exact definition and determination as to the personal data that is necessary to meet the needs and requirements of the legislation. On the basis of Article 38 of the Constitution of the Republic of Slovenia, the nature and extent of personal data provision must be defined by law. The pertinent laws leave that area to be synchronized by statutory provisions in a manner discordant with the Constitution RS. Only the regulator can assess - on the basis of the principle of proportionality - which data is suitable for processing and thus define an admissible intervention into the information privacy of individuals. An act which is hierarchically lower than the law that defines and determines data is also in contravention with the Constitution RS. The Banking Act RS does not define the collection of personal data which is to be processed in the SISBON system and so this issue is left to the content of the Agreement between Banks and Saving Banks. It is even evident from Article 10 of this Agreement that amendments can be proposed by each signatory as well as the Supervisory Board of the Bank Association of Slovenia, and that such amendments come into force when two thirds of the members agree (such a proportion of membership is also calculated on the basis of membership fee remunerated, as opposed to the actual proportion of members). This also means that the collection of personal data which is supposed to be processed in the SISBON system, may well be amended in future for, among other reasons, changes in the offer of banking services pertaining to borrowing, the development of new businesses, system upgrades and inclusion within European credit bureau systems. It is so left to the individual arbitrary assessment of the Bank Association of Slovenia and its members, to decide which personal data will be requested and processed by certain banking subjects (Agreements on the establishment and implementation of the SISBON information system).

Request for assessment as to the constitutionality of the first, second and third paragraphs

19 Official Gazette of the Republic of Slovenia, No. 131/2006 and 1/2008.

of Article 21 of Slovenia's Intelligence and Security Agency Act (ZSOVA)[20] because it lacks the determinability and clarity which would guarantee legal certainty:

The contested provisions do not adequately determine the purpose for which personal data is collected and/or processed. Without a statutorily-determined purpose for processing data it is impossible to ascertain the type and amount of personal data which may be processed in compliance with the law; moreover, it is not possible - within the scope of legal order in the Republic of Slovenia - to satisfy the constitutional request from the first paragraph of Article 38 of the Constitution of RS which mandates that the use of personal data in any manner incongruous with the purpose for which it was collected, shall not be permitted.

This provision namely prescribes that by means of a written decree the director of Slovenia's Intelligence and Security Agency may sanction the monitoring of international communication systems in order to perform Security Agency tasks. The purpose of the collection of personal data pursuant to Article 21 of the Intelligence and Security Agency Act is defined so broadly that - according to the applicant - it would not stand the test of proportionality. The applicant warns as to the double protection of data pertaining to names, telephone numbers and the recording of conversations, which means that any data collected in such manner is not only protected under the provisions of Article 38 of the Constitution of RS but also by Article 37. The content of a conversation or the recording thereof per se, transmitted via any means of communication (e.g. telephone) is primarily protected as communication privacy (under Article 37 of the Constitution RS) rather than information privacy (under Article 38 of the Constitution RS). The right of communication privacy encompasses confidentiality of all kinds of media, and thus protects as confidential any message or conversation transmitted by any means of communication.

3.3. Major Violations of Personal Data Protection

At the beginning of 2008, the Information Commissioner examined a case of inappropriate protection of certain sensitive personal data during transport to the site where said data was supposed to be destroyed. It was established that on the 7th January 2008 near the Slovenska Bistrica junction on the Ljubljana-Maribor motorway, an unidentified number of cardboard boxes, containing internal referrals for laboratory examinations at the Celje Health Centre, fell from a truck en route to the site where these documents were to be incinerated. The cardboard boxes fell apart and their contents – referrals for laboratory examinations which included the personal data of patients – were scattered across both sides of the motorway for some 300 metres. During the investigation it was established that the controller of the personal data Zdravstveni Dom Celje (Celje Health Centre) had entrusted all services related to the removal of personal data (transport and destruction of documents containing personal data) to Pinus TKI, a company which is registered for the collection and disposal of waste materials. Both the health centre and the company were sanctioned for inappropriate protection of personal data (Article 24 and 25 of the Personal Data Protection Act - ZVOP-1-UPB1) and non-compliance with the contractual processing of personal data (Article 11 of the Personal Data Protection). This decision and sanction handed down by the Information Commissioner has not yet become final.

Last year the Information Commissioner examined a case of inappropriate protection of sensitive personal data which received extensive media coverage. During an inspection of the Institute of Oncology in Ljubljana it was established that medical documentation (medical records of deceased patients) were stored in more than a hundred cardboard boxes in an unlocked corridor for a period when construction works at the Institute were in

20 Official Gazette RS, No. 23/99 and pertaining amendments.

progress. It was also established that the records of some patients undergoing treatment at the Institute were stored in two open cabinets in a freely accessible corridor. Sensitive personal data was eminently accessible to all; any passer-by had the possibility of insight into patients' records as well as the opportunity to misuse their personal data. The medical institution was sanctioned for inappropriate protection of personal data (Articles 24 and 25 of the Personal Data Protection Act - ZVOP-1-UPB1). This decision and sanction handed down by the Information Commissioner has not yet become final.

The Information Commissioner established that on 10th March 2008, a group of citizens personally submitted a voter initiative to the mayor of Borovnica municipality; namely, the request for a referendum with regard to the construction of residential property in their municipality. The initiative also included a 52-page list, with signatures, containing personal data on 420 voters who had expressed their support for the initiative. On the same day, Mr. Andrej Doles, a Domžale-based attorney-at-law, authorized to represent the developer Orbital d.o.o., visited the mayor and requested a photocopy of the Initiative and the list of the 420 signatories which contained their personal data. On the same day, the attorney sent a letter to the home addresses of all the signatories in which he called upon them to immediately withdraw their signatures, otherwise claims would be filed against them for damages. The signatories had, allegedly, commercially harmed Orbital, d.o.o., because through signing the initiative they had withheld the release of the municipal ordinance which would have enabled the company to commence the intended construction work in Borovnica municipality.

The Information Commissioner assessed that neither the mayor nor the attorney had the appropriate legal basis which would authorize them to proceed, obtain or use the personal data of the signatories of the voter initiative. Slovenia's Referendum and Public Initiative Act[21] exhaustively prescribes the bodies to which voter data may be entrusted as well as those who may be acquainted with personal data on voters. The law precisely designates those authorities which may have access to the personal data on the voters from the list, i.e. specifically on those who had supported the initiative and called for a referendum. Said authorities are also obliged to protect the personal data provided as confidential (i.e. all data on the signatories save for that pertaining to the individual who instigated the initiative), and, pursuant to the provisions of Article 16 of the Personal Data Protection Act – ZVOP1-UPB1, are not allowed to further proceed or process the data in any way which would not be in compliance with its designated and legal purposes, unless otherwise provided by law.

In compliance with the *Attorneys Act*[22], the attorney was not eligible to either obtain or use the personal data pertaining to voters on the list. He would only be eligible to obtain a copy of the initiative with its original signature (i.e. the identity of the perpetrator and not the endorsees). By giving the attorney the personal data of voters who had supported the call for a referendum, the mayor infringed the provisions of Article 16 of the Personal Data Protection Act – ZVOP-1-UPB1; furthermore, the conduct of both the mayor and the attorney represent contraventions of the first paragraph of Article 38 of the Constitution of the Republic of Slovenia, which explicitly prohibits the use of personal data in a manner incongruous with its provision. This decision handed down by the Information Commissioner has not yet become final, both the mayor and the attorney have filed requests for judicial protection.

The Information Commissioner established that the Minister of Foreign Affairs of the Republic of Slovenia, in relation to the public exposure of a certain document emanating from Slovenia's Embassy in Washington DC, issued an order for a special commission to conduct an internal inspection of the Ministry. Upon a request by the commission, the company Sinfonika provided a list of all incoming and outgoing phone calls made using the terrestrial telephone network at the Ministry of Foreign Affairs. The commission processed the

21 Official Gazette of the RS, No. 15/1994, 38/1996, 59/2001 and 83/2004.
22 Official Gazette of the RS, No. 18/1993, 24/2001.

personal data of the users of the telephones - Ministry employees - in such way that by using a key 'search' in a Microsoft Excel programme, it identified those users who had dialled telephone numbers belonging to a certain newspaper publisher. The commission then used the personal data obtained in this manner for taking further measures within the scope of the internal inspection; namely, the confiscation of personal computers.

The Information Commissioner concluded that by obtaining the list of all incoming and outgoing telephone numbers from the Ministry's terrestrial telephone network over a certain period (around 110,000 records), the personal data of employees and the personal data of those persons with whom said employees had communicated had been collected illegally; further to which the commission's processing of such data was in contravention of the provisions of Articles 8 and 16 of the Personal Data Protection Act. There was no valid reason for obtaining and using the records of incoming and outgoing phone calls, further to which the document in question (a dispatch) may not be transmitted to unauthorized persons by telephone. The mere fact that an employee of the Ministry contacted a telephone number belonging to a certain newspaper does not represent any sort of proof that the individual in question actually conveyed a copy of document to a newspaper publisher. In this instance we witnessed two infringements, namely: the illegal processing of personal data and the commissioning of a subcontractor - Sinfonika - to create a data filing system of all Ministry employees from the data contained in the in-house telephone exchange system, without having signed a contract for such an operation within the meaning of Article 11 of the Personal Data Protection Act.

The Information Commissioner established that the Competition Protection Office of the Republic of Slovenia (hereinafter CPO), within the scope of its investigation of a retail company, had copied the entire hard-disks of some personal computers, which also contained personal data and the personal correspondence of employees of the retail company. According to the CPO, the legal basis for the copying of hard disks was provided by Article 29 of the *Prevention of Restriction of Competition Act*[23] which upholds that authorized persons may confiscate or obtain copies or extracts from business books or other business records of a company or an office, in any form, namely by using photocopying devices and computer equipment. The CPO expressed the opinion that the entire documentation, located at the premises of the retailer, shall be regarded as business records, regardless of the data carrier on which it is recorded.

By means of a Decision, the Information Commissioner prohibited the CPO from using (accessing, copying, transferring…) certain personal data in electronic form, which the latter had obtained within the scope of the investigation conducted in relation to three retailers. The media, which the CPO obtained and created during the conduct of the procedure, also encompassed data in relation to the email contacts and correspondence of employees. Such data encompassed sent and received emails (email address, date and time, sender, recipient and subject matter), data on contacts in personal address books as well as entries into calendars. In the copying of the entire content of hard disks, user profile data was also copied together with data on the use of electronic mail. User profile information - namely data that is created when using the Internet, including data on accessed websites, cookies etc. - is stored in a special file on the hard disk of a computer, and as such it contains data which should be regarded as personal to the user. Under no circumstances can such data can be regarded as information originating from or pertaining to business records, hence there is neither appropriate legal basis for its processing or compliance with the provisions of Article 8 of the Personal Data Protection Act.

If both the nature of the personal data retrieved and its processing were stipulated by law, the CPO would only be permitted to process the personal data using the media created in manner concordant with the provisions of the first paragraph of Article 9 of the Personal Data Protection Act. The Information Commissioner concluded that Article 29 of the Prevention of Obstruction of Competition Act does not provide sufficient legal basis in itself

23 Official Gazette of the RS, No. 36/08.

for the retrieval of electronic mail or the opening of same for the purposes of inspection or use of the personal data which forms a constituent part of said electronic mail.

Copying, opening, inspecting and using the electronic mail of an individual represents an intrusion into the privacy of that person, namely into the right to privacy of correspondence as well as so-called communications privacy. Because this right is also derives from Article 38 of the Constitution of the Republic of Slovenia, which protects the privacy of information and data communicated by e-mail, the confiscation of such documentation represents the illegal processing of personal data.

The Information Commissioner also examined how civil servants respect personal data protection in various public administration registers, and specifically eligibility as regards access to the register of taxpayers. Based on the principle of traceability, which has been facilitated by the Tax Administration of the Republic of Slovenia, as the personal data controller in compliance of the Personal Data Protection Act, the Information Commissioner consulted the computer database on all accesses (insights) into the register for 15 well-known holders of public office in Slovenia. The Tax Administration of RS provided a list of employees who had consulted the data on the designated individuals between 1st January and 31st August 2008. This process established that of the 200 employees who had accessed these files, only 47 employees had consulted the specific registers in accordance with the sole legally permitted purpose, i.e. conducting a tax procedure. The remaining 153 employees who accessed these files had no justifiable reason for their action. The most common reason for gaining insight was mere curiosity; the employees of the Tax Administration of RS were checking the age or address of well-known Slovenes. Processing personal data without an appropriate legal basis, is a violation of Article 8 of the Personal Data Protection Act, further to which the Information Commissioner issued a warning as a caution to other civil servants, reminding them that they are not permitted to 'browse' through the data without a legal basis for such action.

3.4. Overall Assessment and Recommendations Regarding Personal Data Protection

Observations in 2008 revealed the same or similar violations and irregularities concerning personal data protection as in previous years. In the majority of cases, irregularities emanated not as a consequence of deliberate violations of the law, but, above all, as a consequence of the poor knowledge of data controllers as to the provisions of the Personal Data Protection Act, or a mere lack of attention dedicated to the protection of personal data.

The introduction of the Act Amending the Personal Data Protection Act (ZVOP-1A) engendered some changes and innovations, including the exception to the obligation of establishment and upkeep of personal data collection catalogues, (Article 26 of the Personal Data Protection Act) as well as transferring data from catalogues to the register (Article 27 of the Personal Data Protection Act) for all the data controllers which had fewer than 50 employees; however, such exception does not apply to all data controllers in the public sector.

Pursuant to the fifth paragraph of Article 7 of the Personal Data Protection Act – ZVOP1-UPB1, such regulation does also not apply for notaries, lawyers, detectives, bailiffs, executors of personal protection, private health care and medical service providers, together with the controllers of personal data whose collections include sensitive personal data. Through the implementation of the aforementioned innovations, the Personal Data Protection Act has actually placed more burdens upon the later private sector data controllers (notaries, lawyers, detectives, etc.) since they now - in compliance with the law - also have to provide catalogues for the data filing systems they administer in relation to their employees,

something which they had not previously been obliged to do if they had fewer than twenty full-time workers.

The Information Commissioner establishes that the situation regarding the administration of catalogues and registers during this period has improved significantly; there still remain, however, numerous violations in this area.

Consequent to its inspection procedures regarding video surveillance, the Information Commissioner establishes that the most common irregularities in relation to video surveillance are as follows:

- Notifications still all too frequently did not include all the information prescribed by law, or were too small in size and displayed in inappropriate places.
- Managers failed to provide written notification as to any decision to instigate video surveillance, either before or following its implementation, as well as failed to list the reasons for its implementation in any such written notification.
- Employers failed to provide employees with written notification as to video surveillance prior to its implementation. In many cases it was established that the surveillance providers failed to initiate a personal data collection catalogue in relation to the surveillance system register, and further failed to submit data from the catalogue to the Information Commissioner.
- In many instances the controllers of video surveillance systems failed to keep records of the inspection of recordings, so it is not possible to determine who was inspecting certain recordings for a particular period, as well as for what purpose the inspection of video records were carried out.
- Most problematic in the implementation of video surveillance in multi-occupation buildings was the manner in which live recordings were simultaneously relayed via an especially dedicated cable television channel available within the building.

When assessing compliance with the provisions of the Personal Data Protection Act in relation to direct marketing, it was ascertained that in order to send advertising materials and commercial offers more often than not personal data contained in publicly accessible filing systems or personal data acquired within the framework of the lawful performance of activities was being used. These public filing systems encompassed such records as telephone directories, share registers, as well as land and cadastral registers. Merely taking data from these collections did not violate the provisions of the Personal Data Protection Act; however, violations did occur through the utilization of personal data pertaining to persons injured in traffic and other accidents who had been transported to hospital. It involved companies operating in the field of insurance claim consultancy and mediation in the payment of insurance claims, and information leaflets offering such services were sent to the home addresses of individuals who had been taken to hospital. The personal data of hospitalised persons were by no means obtained from publicly accessible sources, and hence the Information Commissioner instigated offence proceedings against the companies and persons responsible. The Personal Data Protection Act was violated in relation to the use of personal data collections for direct marketing in a manner where more personal data than is permitted by law was used. Further to this, the direct marketers often failed to inform the individuals they contacted of their statutory right to demand - at any time and 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. There were also recorded instances where data controllers kept sending advertising materials to individuals who had specifically requested that they should not be the recipient of any more such materials.

In relation to the direct collection of personal data, it should be stated that personal data controllers all too often fail to convey all the information stipulated by Article 19 of the Personal Data Protection Act to the individual, or that such information - e.g. data on the controller of personal data and a clearly defined purpose for processing, information on potential users of personal data and the information on the right to insight, transcript, copy, amendment, correction, blocking or deletion of one's own personal data - is incomplete. Provision of information during the collection of personal data is particularly

important when personal data is processed upon the personal consent of an individual, because that person is only able to decide whether or not they will permit the processing of their personal data if they receive the complete information. All too often the purpose of personal data processing is defined too broadly, or not defined at all.

With regard to transferring personal data from personal data collections to other users, the Information Commissioner establishes that personal data is all too frequently supplied or disclosed to unlawful users; namely, those who are not authorized for the collection of personal data either by law or by personal consent of the individual to whom the data pertains. In relation to this, the most common irregularity appears to be the fact that the supply or transfer of personal data is not in any way recorded, or that the records are incomplete. Article 22 of the Personal Data Protection Act namely provides that as regards any supply or transfer of personal data, the data controller shall be obliged to ensure that it is subsequently possible to determine - consequent to the proscribed supply of personal data -the nature and extent of the personal data supplied, when, to whom, and on what basis, for the period covered by the statutory protection of the rights of an individual.

Irregularities pertaining to personal data protection were also a consequence of deficient internal acts implementing organisational procedures, methodologies and measures to protect personal data in relation to the obligation of data controllers laid down in Articles 24 and 25 of the Personal Data Protection Act. In relation to this, it should be stressed that it is not enough to merely prescribe personal data protection measures and procedures in internal regulations: it must be ensured that they are carried out. For this very reason all employees should be familiarized with the acts which prescribe personal data protection procedures and measures, besides which, pursuant to Article 25 of the Personal Data Protection Act ZVOP-1-UPB1, data controllers shall define the persons responsible for individual filing systems as well as those who, due to the nature of their work, administer the actual data. Some data controllers are presently not governed by internal regulations and, where such regulations do exist, many of those who were processing personal data are unfamiliar with them.

During their inspections, national Supervisors for personal data protection found documents containing personal data in unlocked cabinets and drawers, as well as in corridors and in other unlocked premises; computer equipment and software used for processing personal data were likewise unprotected. Insufficient traceability, or a lack of traceability in the processing of personal data, was also all too frequent, and as regards this problem the Information Commissioner became particularly involved in public sector supervision, and specifically so as regards the health service. In relation to the protection of personal data, which has to be commensurate with the risk represented by processing, special emphasis should be placed on the obligation to protect personal data in relation to the supervision of its proper deletion or destruction.

The Information Commissioner establishes that the submission of applications in relation to complaints against employers who monitored electronic mail and required medical data from their employees is increasing year by year. Email monitoring, in itself, represents a conflict of interests. On the one hand employers have an interest in and a right of control over their assets, as well as the according right to monitor whether their equipment is being used for the purpose(s) for which it was provided an employee; at the same time, however, the individual employee rightfully expects that they might enjoy a certain degree of privacy and confidentiality within the workplace. In principal, the employer has no legal grounds to look into so called traffic data in relation to the email of its employees, namely: the identification of senders and recipients of emails or the content thereof. In accessing such data, an employer simultaneously violates the employees' right to personal data protection, and by monitoring email violates the right to privacy - in its broadest sense - as well as the right to confidentiality of communication; both of these rights are protected by the Constitution RS.

There were several applications pertaining to an employer's request for access to the medi-

cal records of employees and inspection during their sick leave. The Information Commissioner emphasizes that employers are very restricted when it comes to the access of sensitive medical records. Employers are not entitled to familiarization with any diagnosis as to the health or medical conditions of individual employees; however, an employer is entitled to examine the justification for an employee's absence - either themselves or through the use of an authorized detective, in accordance with the Detective Activities Act - namely, to corroborate the actual existence of illness and the regime of movement (but not the regime of treatment). It is hence of key importance that employees respect the instructions provided by their physicians re rest regimes and permitted movements in relation to any mandated period of absence from work. Without data as to how much an employee is able to move around and how much they have to rest, an employer is unable take appropriate measures in cases of suspicion of abuse of sick leave.

Despite all the above stated irregularities, the Information Commissioner establishes that the controllers of personal data as well as the individuals are by the year becoming increasingly aware as to the significance of personal data protection, which is also reflected in a rising number of applications pertaining to suspicion of abuse of personal data and a high number of requests for opinions, clarifications and recommendations which data controllers are addressing to the supervisory authority on a daily basis. For the purpose of raising broader awareness as to the importance of personal data protection as a narrower segment of the right to the protection of privacy, the Information Commissioner dedicates a deal of attention to the education of controllers of personal data collections as well as other individuals. For this purpose, the Information Commissioner organizes courses, participates in a variety of panel discussions and issues a great many expert articles and clarifications for publication.

Among the key measures in the field of prevention activities is Privacy Impact Assessment, which is particularly important in cases of larger projects and amendments to legislation, and reflects the opinions of the Information Commissioner on proposals of amendments to legislation, as well as its reactions to projects which envisage the extensive processing of personal data. Such assessments are the foundation of the concept of Privacy by Design, which envisages care for the protection of privacy in all phases of a project which embraces the processing of personal data. Privacy impact assessments are of key importance in the initial phases because the retrospective solution is often time consuming and requires radical alterations of the system's concept, which in itself engenders considerable costs. Further to this, the Information Commissioner shall issue a privacy impact assessment methodology manual in 2009.

The Information Commissioner observes that liable persons all too often solely dedicate a deal of attention to technical measures and mechanisms for the protection of personal data, whereas appropriate organizational measures and procedures are being ignored. The latter are particularly important when the organizational measures must ensure that the personal data, controlled by a liable person, is used in compliance with the purpose of use. This is particularly important in larger public sector collections, where the use of personal data for private purposes or for purposes other than those for which such data was initially collected, is prohibited. It should be pointed out that mere insight into or access to personal data represents the processing of personal data, for which a legal basis is mandatory.

In 2008 the Information Commissioner commenced an investigation into the purposes and use of public sector personal data filing systems, and observed that more attention should be dedicated to organizational measures for the protection of personal data which need to accompany technology-based methods and procedures. Of particular concern is the adoption of appropriate measures and acts for raising employee awareness, as well as internal controls which will minimize the possibility that those employees who are provided to have access to personal data in the scope of their tasks and competencies, will not do so for prohibited and illegal purposes. Any detected violation must be sanctioned for the very reason it raises awareness and respect for the legislation among other employees.

As a result of observations made during inspections, together with ongoing endeavours to improve the situation in the field of personal data protection, the Information Commissioner also concedes that it will have to pay more attention to preventive action, in the scope of which are the provision of educational activities; at the same time, awareness-raising among data controllers who are responsible for personal data processing, will also have to be improved. Within its jurisdiction and in co-operation with experts, the Information Commissioner will be able to prepare and publish for the attention of data controllers non-mandatory written instructions and recommendations with regard to those issues and areas that are most frequently a source of irregularities. As part of its pre-emptive activities, the Information Commissioner will need to invigorate its preventive inspections in those spheres - and with those data controllers - which hold several personal data collections or who process sensitive personal data. These include, in particular, data controllers in the fields of healthcare, social security and insurance operations, together with large employers, state, municipal and local authorities, public service sector providers as well as other public sector operators.

The legislator - and specifically those responsible for drawing up legislation - will also have to pay more attention to the normative regulation of personal data protection. During 2008, the Information Commissioner submitted a great deal of commentary on proposed legislation; in most instances the objections raised refer to the disproportionate collection of personal data as well as an insufficient definition as to the purpose. When preparing statutes regulating the processing of personal data in individual sectors, particular attention shall have to be paid to the principle of proportionality; namely, sectoral law should only impose the processing of data germane to the scope of its absolute objective. The Information Commissioner is still observing that in practice the regulation of personal data protection is carried out by way of ancillary regulations which are unlawful due to the very fact that they are discordant with the Constitution RS, the provisions of which state that the types of personal data which shall be applicable shall be specifically prescribed by law. Namely, pertinent legislation has to clearly stipulate what personal data may be processed as well as the purpose(s) for which it may be used, whereby said purpose(s) must be constitutionally admissible. If the personal data collected is to be determined by way of ancillary statute, the door is open to arbitrary assessment as to what data may be collected by the authority authorized to instigate such regulations. The Information Commissioner also recommends that new legislation clearly stipulates the maximum period of retention for personal data thus processed.

The Information Commissioner also reprimanded the legislator for its unwarranted intervention into the privacy of the person. Namely, in some instances legislation has been adopted too hurriedly, without due consideration and appropriate risk assessment as to infringements upon the privacy of the individual. However, the situation in this area is improving; ministries frequently co-operate with the Information Commissioner in the preparation of legislative provisions which prescribe personal data processing in individual areas.

In this era of the information society, the processing of personal data cannot be imagined without integrating or merging data filing systems. Such certainly facilitates the management of personal data filing systems by data controllers, and when merged with the so-called original data filing systems, for example the central population register, they can provide accurate and updated personal data. At the same time, however, this practice can lead to the establishment of large centralized data filing systems, from which one can obtain an almost indefinite amount of data in one location which is administered in various data filing systems for numerous purposes by different controllers. With regard to the increased amount of abuse, the Information Commissioner as well as the various legislative authorities will have to dedicate more attention to this particular area.

When preparing the legal framework, legislators shall have to assess whether the integration of data filing systems is absolutely necessary in order to achieve the constitutionally admissible purpose. Prior to any actual integration, the Information Commissioner is likewise obliged to diligently examine whether there exists an appropriate legal basis for any

anticipated integration of data filing systems, as well as examine whether data controllers provide appropriate security. Data controllers will have to vindicate that they strictly respect and abide by the provisions of the Personal Data Protection Act, which means that they will be obliged to inform the Information Commissioner thereof in writing prior to the integration of data filing systems. Those data controllers who are already integrating data filing systems will have to record information on integrated data filing systems in their catalogues of data filing systems and transfer same to the register of personal data filing systems.

The information Commissioner observed that neither the controller of the tax register (Tax Administration RS), nor the controller of the central population register (Ministry of Internal Affairs) had reported the data on integrated data filing systems into the register of personal data filing systems, although it is widely-known that these two personal data filing systems are integrated with other filing systems and with each other. In relation to the integration of personal data filing systems, attention is drawn to the legal vacuum within the Personal Data Protection Act, since said Act does not define what the integration of data collection means. Because practical dilemmas arise in relation to the question of differentiation as to the integration of personal data and its mere provision, the Information Commissioner has prepared an appropriate clarification which is now published on its website.

The situation as regards personal data protection in Slovenia's healthcare sector is improving; however, the Information Commissioner is still receiving a great many complaints, most of which pertain to the inappropriate protection of sensitive personal data. Special attention is being dedicated to the transfer of sensitive personal data, especially via telecommunications networks, since the law in such instances requires that data is rendered illegible and/or unrecognizable by means of cryptography and mandatory electronic signature. The Information Commissioner has warned data controllers on several occasions that they must protect sensitive personal data in the prescribed manner during any telecommunications transfer. More attention will also have to be dedicated to the physical protection of medical records (appropriate filing cabinets in appropriately secured premises), restricting the circle of people who have access to certain personal data and the provision of improved traceability of personal data processing, whereby such measures will also prevent the use of personal data for unwarranted or illegal purposes.

During the course of 2008, the Information Commissioner was again warning as to the significance and subtlety of the introduction of biometric measures. Every controller of personal data who intends to perform biometric measures is obliged - prior to their introduction - to submit to the Information Commissioner a description of the intended measures, as well as the reasons for their implementation. In order to avoid wasted upfront costs, namely prior to any purchase of a biometric reader, the Information Commissioner warns that any controller who wishes to introduce biometric measures should first file an application for a decision by the Information Commissioner, which shall determine whether or not such introduction of biometrics is legally admissible. On numerous occasions in practice controllers have invested in a reader only for the Information Commissioner to establish that the proposed implementation was not in compliance with the law, and accordingly no pronouncement consenting to the implementation of biometric measures was provided because it turned out that such were not indispensable for carrying out mandatory operations, or for the security of people or property, or for the protection of confidential data and business secrecy.

Last year, the Information Commissioner dedicated a deal of attention to the vexed question of employee expectations of privacy in the workplace, especially related to the use of corporate email, telephones and computers that are, to some extent, also used by the employees for private purposes. The Information Commissioner hence recommends that employers should precisely describe any procedures and measures which could potentially represent an intrusion into the privacy of employees; and furthermore such should be undertaken in advance through provisions laid down in the organization's internal statutes, accordingly acquainting employees beforehand and thus avoiding situations that would

otherwise represent an unwarranted intrusion into employee privacy. Namely, employees shall not be obliged to waive the right to privacy at work in its entirety, but the Information Commissioner recommends that employers draw up precise written instructions that define the circumstances in which intrusions into the privacy of an employee may be warranted. Every such intrusion, defined in advance, must also, of course, be legal and acceptable in respect of constitutionally enshrined rights. Regarding the fact that the sphere of privacy in the workplace is under regulated, the Information Commissioner considers that this area should be more precisely defined by law.

In 2007 Information Commissioner commenced writing guidelines for all those areas and issues, which were proving to be the most problematical, and these were then published on its website. In 2008, the Information Commissioner published all legal opinions, remarks regarding legislation, requests for assessments as to constitutionality and relevant decisions on its website, and addressed a special recommendation to individuals and the controllers of personal data filing systems - indeed anyone and everyone who has any questions relating to personal data protection - to first examine the resources now available through the website, where a great possibility exists that the answers to questions will be found.

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 filing system 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 15 acts of parliament and other legislative regulations during 2008, and was also involved in two cases at the European Court of Justice in Luxembourg.

4.2. Relationship with the Media

By way of comments and interviews, press conferences, press releases, statements, as well as through its own website, the Information Commissioner regularly uses media to engage in awareness-raising among legal entities as well as the public at large.

In 2008, the Information Commissioner yet again endeavoured to provide the very best web pages in Slovenia, and was rewarded with a Golden Netko Award for the best website in the state and public administration and associations category. This website is used as a medium for reporting violations pertaining to the protection of personal data, and at the same time offers a simple access to a great number of opinions, decisions and other public information in relation to personal data protection.

The second European Personal Data Protection Day was marked by a multimedia discussion organised by the Information Commissioner which was dedicated to the theme of safe use of the Internet and other state-of-the-art technologies used by young people in relation to the safety of personal data on the Internet. The occasion was also marked by the publication of a pamphlet entitled Only You Decide; intended for young people, parents and teachers, it warns of the pitfalls of personal data abuse on the Internet. The Information Commissioner also presented two awards - one for a public sector operator, and one for a private one - for good practice in the field of personal data protection during 2007.

The Right to Know Day, which has been celebrated on 28th September each year since 2002 and which marks the principle of openness and transparency worldwide, saw Slovenia's Information Commissioner play host fellow commissioners from European countries. Participants at the Third European Conference of Information Commissioners on 29th September 2008 exchanged their experiences and discussed issues of the effective, practical and - moreover - rapid exercise of the right to access public information. The occasion of the fifth anniversary of its operations and the adoption of the Access to Public Information Act was also marked by the Transparency? Yes Please Award.

The Information Commissioner provides education for liable persons and entities through its organization of a variety of workshops and seminars; further to which purpose a number of conferences and panel discussions were also organized.

Among the Information Commissioner's prevention activities are the issue 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. During 2008, the Information Commissioner issued the following guidelines which are accessible via the Internet:

- Guidelines for the protection of personal data in hospital information systems

- Guidelines in the introduction of biometric measures
- Guidelines for personal data protection in employment relationships
- Guidelines for carrying out video surveillance.

In 2008 the Information Commissioner published its Annual Report for 2007.

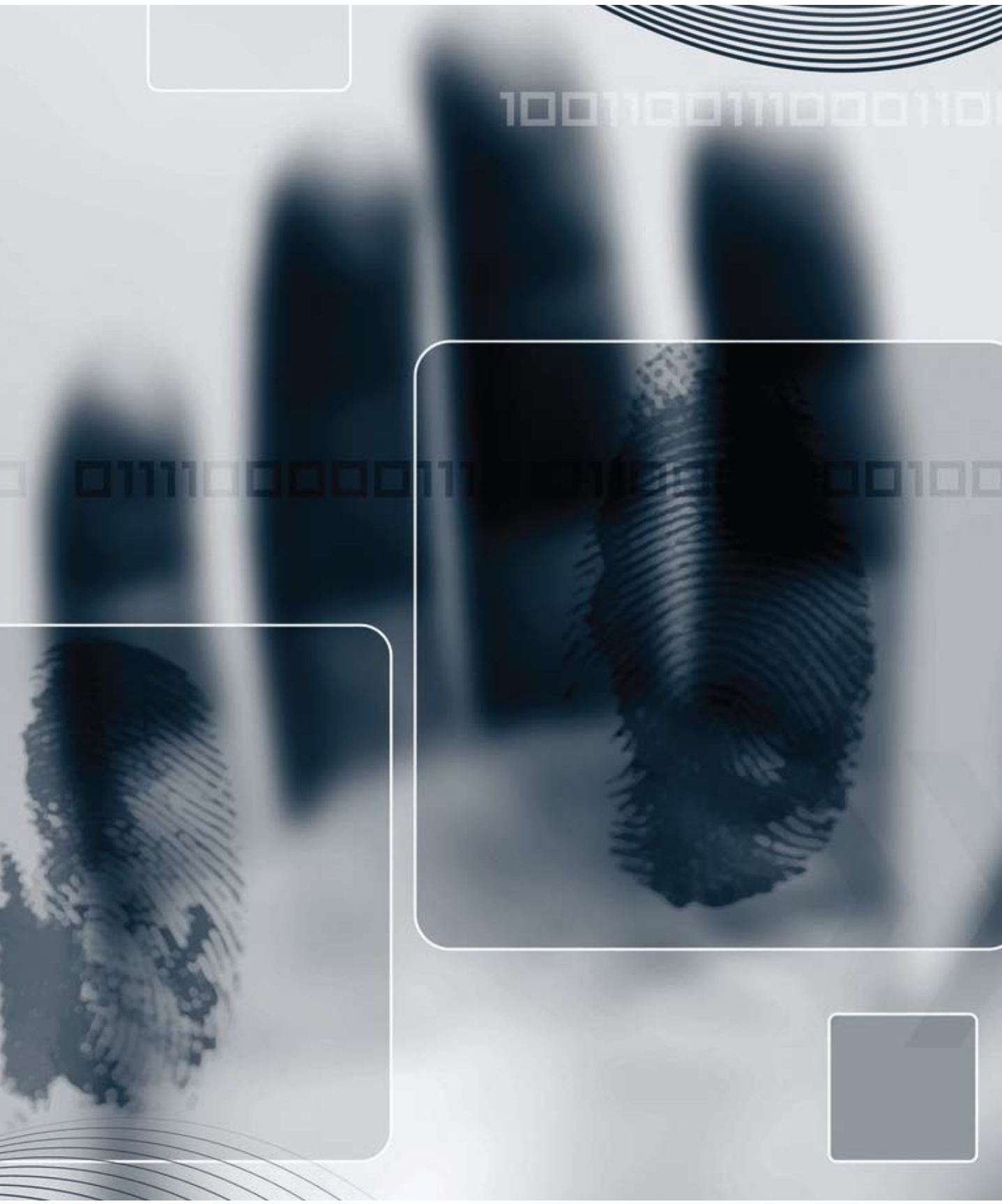
A Slovene survey entitled Politbarometer conducted by the Center za Raziskavo Javnega Mnenja (Public Opinion Research Centre) for the first time also included the Information Commissioner in its December 2008 survey into what extent do people trust institutions. The results revealed that 47% of respondents trust the Information Commissioner, which placed it in fourth place after the President of the Republic of Slovenia (55%), the Euro (53%), and the Bank of Slovenia (49%). The Politbarometer survey also included a question in relation to untrustworthy institutions, whereby the Information Commissioner achieved second best place (respondents gave fewer negative marks only to the school system) in front of 22 other institutions which were included in the survey. The high level of trust in the Information Commissioner points to the significance and the need for this independent body.

The Information Commissioner dedicates a lot of attention to preventive actions, especially education and awareness-raising among controllers of personal data collections as well as other individuals. We were delighted at the results of the Eurobarometer public opinion survey into public awareness, opinions and views as to personal data protection: in this survey of EU citizens, Slovenia is placed at the very top of the community's 27 member states as regards public appreciation of the problems and issues of data protection.

4.3. International Co-operation

During 2008 Information Commissioner employees took part in 19 international seminars and conferences, and they presented their own contributions at three of these events.

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. These encompass: the working group for the protection of personal data under Article 29 of the European Data Protection Directive (95/46/EU), the joint supervisory bodies for Europol (European law enforcement), the Schengen area and the customs information system, as well as the co-ordination meetings of the European Data Protection Supervisor (EDPS) together with national bodies for the protection of personal data. The Information Commissioner also actively participated in the Internet and Information Technology Sub-Group under the auspices of the European Data Directive Working Group, whilst within the scope of police and judicial co-operation it also regularly attended meetings of the Working Party for Police and Justice (WPPJ). The Information Commissioner was also active in the IWGDPT – International Working Group on Data Protection in Telecommunications, 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).



Annual Report prepared by:

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

Andrej Tomšič, Deputy Information Commissioner

Translation:

Ars Lingue, Tina Mušič, MA

Ljubljana, Slovenia, July 2009