Information Commissioner Annual Report

2007

REPUBLIC OF SLOVENIA

INFORMATION COMMISSIONER

'07 Information Commissioner Annual Report

2007

0 INTRODUCTION

The right of freedom of expression and the right to protection of privacy are upheld and safeguarded by the Information Commissioner as an independent organ of the state. As fundamental pillars of democracy, both of these rights intertwine in the work of Slovenia's public sector as well as the everyday life of the people, and hence they contribute to development of the rule of law.

Adoption of the Information Commissioner Act has enabled the co-existence of the right to freedom of expression and the protection of privacy. Co-ordinated interpretation and a considered approach to both legal domains is exceptionally important in the legal protection and - in particular - for an awareness that the mission of the Information Commissioner is commensurate with the upholding of both of these basic human rights.

In accordance with Article 14 of the Information Commissioner Act, the Information Commissioner has prepared a report as to its work during 2007, which was accordingly submitted to the National Assembly - the parliament of the Republic of Slovenia - in May 2008; this year's report, our second, marks two years of work. I am pleased to have established that the level of respect and awareness as to the importance of freedom of expression and the right to protection of privacy is becoming greater each passing year; however, we should not be satisfied with the level thus far attained.

Good sectoral laws have facilitated the effective operation of the Information Commissioner, further to which Slovenia's Access to Public Information Act can be regarded as one of the best in the world; indeed, many countries have used it as a model, especially those which have yet to introduce legal regulation of this area. The Personal Data Protection Act also contains all the elements pertaining to control and inspection, which the supervisory authority needs to carry out its work appropriately. However, without the sincere commitment and diligent work of Information Commissioner employees, and a concordant response to suspected infringements of the aforementioned human rights, laws and acts would remain mere dead letters on paper.

The Information Commissioner enjoys the cordial co-operation of all organs of the state, and thus the need to resort to negative exposure never arises. Expert arguments, expressed in remarks to legislation and statutory procedure, contribute to a improved regulatory processes and the enhanced institution of human rights.

During 2007 the Information Commissioner issued a number of publications and guidelines pertaining to those individual areas that were proving to be the 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. Information Commissioner experts also participated in numerous informative conferences, congresses and panel discussions over the course of the year, and, during 2007, also marked the Personal Data Protection Day and the 5th Right to Know Day.

Particular attention was dedicated to those issues emanating from the rapid development of information-communication technology. Such developments undoubtedly make everyday life easier; however, at the same time they enhance the potential for intrusion of privacy, per se, as well as the abuse of personal data. New technologies and new services such as RFID (Radio Frequency Identification), RuBee, biometrics, surveillance and similar such technologies which may be applied to a location or the movement of an individual, represent new threats, in particular to the privacy of the individual. In an environment of omnipresent inter-connectable technologies we are increasingly less aware as to how, when, where and by whom our personal data is being processed, and hence the possibility of abuse of personal data, whereof the person concerned may not necessarily ever become aware, is heightened.

In order to improve information provision, the Information Commissioner website has been redesigned and is now more user-friendly for both expert as well as lay publics. All legal opinions and decisions pertaining to personal data protection have been published in order to raise public awareness.

Due to the increased scope of our work and new responsibilities, together with enhanced international engagement, the number of Information Commissioner employees - in particular the number of National Supervisors of Personal Data Protection - has increased. As of 1st January 2007 the Information Commissioner had 25 employees, which had risen to 29 by year's end.

I shall continue to strive for the work of the Information Commissioner to be recognizable, both in Slovenia as well as abroad.

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

INTRODUCTION

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

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

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 decision. The silence of an authority in such an instance is an offence, as well as grounds for a complaint. A complaint against a rejection is permitted if the negative reply to the question pertains to a document, case, file, register, record or other such archive. The Information Commissioner makes a decision as to a complaint against a rejection decision under the provisions of the Act on the Access to Information of Public Character[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[4].

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 the second paragraph of Article 112 of the Electronic Communications Act[5] (ZEKom), 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.

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

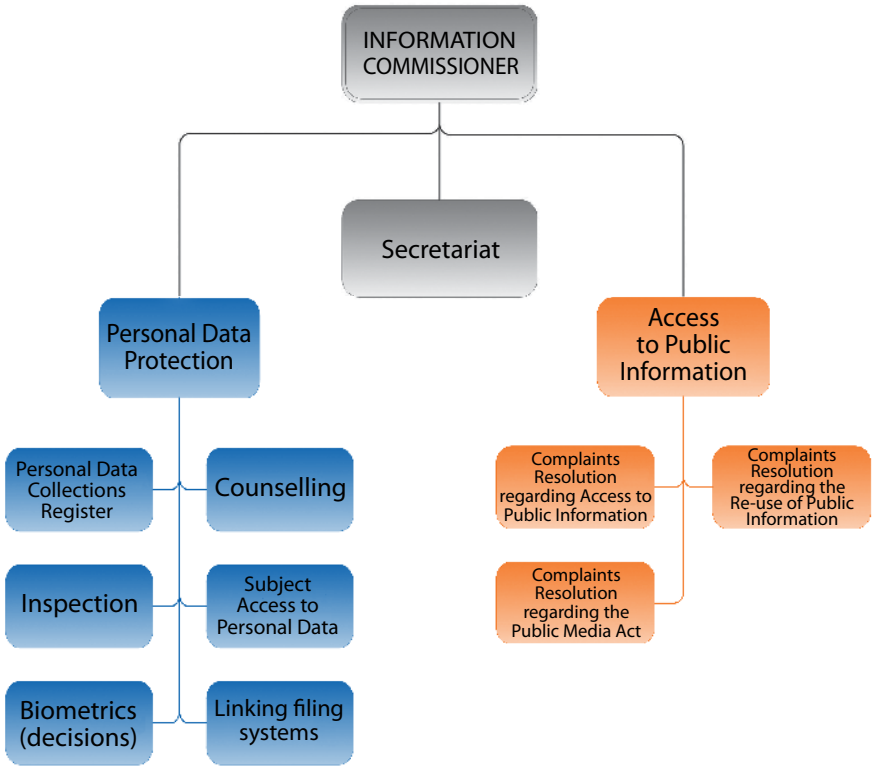
[2] Official Gazette of the Republic of Slovenia, No. 110/2006, official consolidated text.
[3] Official Gazette of the Republic of Slovenia, No. 51/2006, official consolidated text and 117/2006-ZDavP2.
[4] Official Gazette of the Republic of Slovenia, No . 86/2004 and 113/2005-ZInfP.
[5] Official Gazette of RS, No. 13/2007 - Electronic Communications Act (ZEKom).

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 2006; and in particular the number of National Supervisors for the personal data protection rose. On 1st January 2006 the Information Commissioner had 15 personnel; this number had risen to 25 by year's end. All those working as civil servants within the organisation have university degrees, 4 with a masters degree, and 1 with a doctorate.

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 2007, this allocation amounted to the equivalent of 1,220,007 euros, rising to 1,249,060 euros at year's end. During fiscal 2007, the Information Commissioner had spent 1,237,544 euros, namely:

- 806,188 euros for salaries and other employee expenses;
- 354,027 euros in material costs;
- 77,328 euros in investments and capital expenditure.

Accordingly, 99.64 % of the available budget for 2007 had been used during the course of the year.


INFORMATION COMMISSIONER

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[6]. 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[7]. 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.

Two new pieces of legislation - the Public Procurement Act[8] and the Market in Financial Instruments Act[9]) - both of which limited the Access to Public Information Act, were adopted during 2007. Said Acts expand the exceptions to freely accessible public information and hence interfere with the already established system of transparency, and in particular clarity re exceptions in accordance with the Access to Public Information Act.

2.2. Review of Activities in the field of Access to Public Information during 2007

121 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 2007. The Information Commissioner issued 83 decisions, 9 cases were carried over from 2006. The number of decisions in the field of access to public information was slightly down on the number recorded in 2006.

6 Official Gazette of the Republic of Slovenia, Nos. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006 - the Constitution of the Republic of Slovenia.

7 Official Gazette of the Republic of Slovenia, No. 24/2003.- Access to Public Information Act (ZDIJZ).

8 Official Gazette of RS, No. 128/2006 - Public Procurement Act-2. (ZJN-2).

9 Official Gazette of the Republic of Slovenia, Nos. 67/2007 and 100/2007 Market in Financial Instruments Act. (ZTFI).

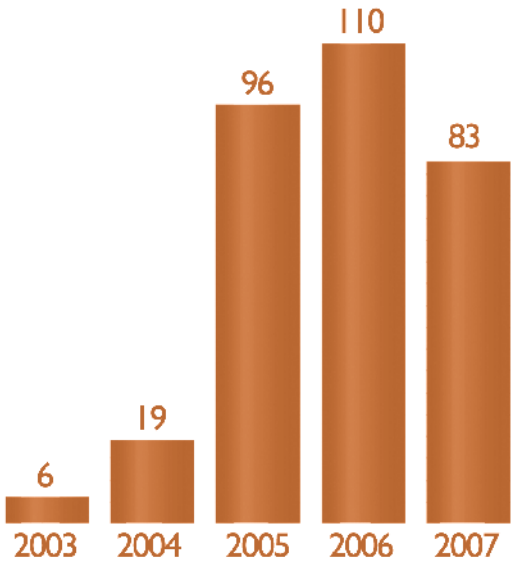


Diagram 2:

Number of decisions handed down in relation to access to public information, 2003-2007

As regards the decisions the Information Commissioner:

- resolved the matter in favour of the applicants in 46 cases
- rejected the complaints in 24 cases
- partially approved access in 9 cases, and
- returned the matter to the first instance authority in 4 cases.

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 Public Information Access Act (30);
- whether the requested document included personal data, the disclosure of which would contravene the provisions of the Personal Data Protection Act (28);
- whether the applicant requested information and/or data considered a business secret, according to the act regulating companies (14);
- whether the liable person or authority holds the document or the public information which has been requested by the applicant (9);
- whether the authority, to which the request for public information was addressed, is liable to provide information in accordance with the Access to Public Information Act (6);
- 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 (4);
- whether the requested information is data pertaining to documents still under preparation and thus subject to internal consultation, further to which premature disclosure could result in misinterpretation as to their content (3);
- 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 (3);
- 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 (3);

- whether the requested information contained data that was classified (as an official secret) on the basis of the law regulating classified data (2);
- 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 (2);
- 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 (2).

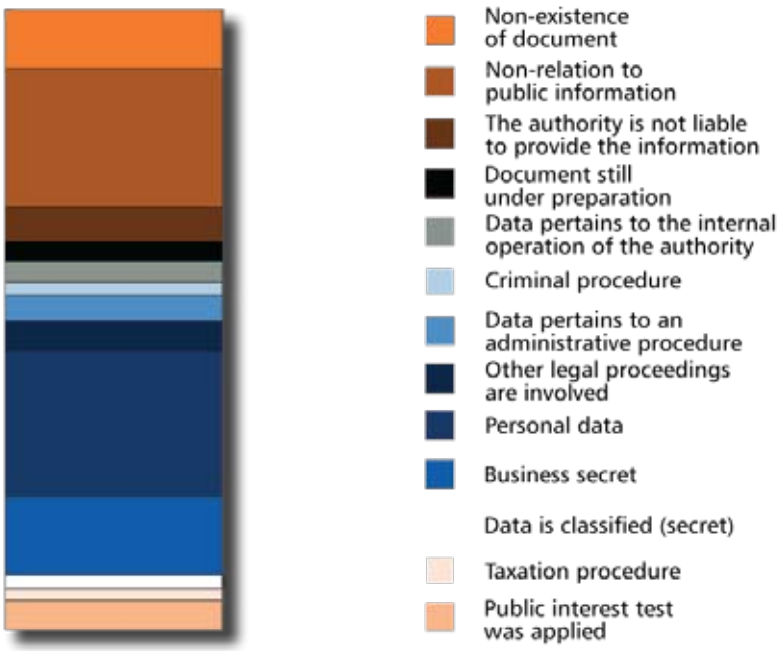


Diagram 3: Decisions taken in relation to the Access to Public Information Act with regard to various exemptions (N.B. a single decision may refer to several exemptions).

Complaints lodged by applicants as the result of a rejection of access to public information concerned the following groups of liable authorities:

- Ministries and their constituent bodies (35);
- Public funds, institutes, agencies and other entities subject to public law (30);
- Educational institutions (25);
- Administrative units and municipalities (14);
- Courts and the State Prosecutor's Office (13);
- Health authorities (3);
- Ombudsman of the Republic of Slovenia (1).

46 applications were lodged by private individuals, in 33 instances the applicants were journalists and on 20 occasions NGOs, various associations and societies. In 21 instances private sector legal entities, including entrepreneurs and law firms, lodged complaints as to the lack of provision of requested information; the Information Commissioner also received one complaint by a municipality.

In 2007, 12 lawsuits were filed at the Administrative Court against decisions made by the Information Commissioner, a figure which represents 13% 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 2007, the court had only handed down a decision as to one of the aforementioned lawsuits, and it was rejected. As of the end of 2007, the Administrative Court RS had rendered 29 judgements on decisions from previous years. In 14 instances the contested decision was annulled and the matter returned to the Information Commissioner for reconsideration; in 3 cases the suits were partially granted, and in 12 cases the Administrative Court rejected the complaints. In 2007 the Supreme Court decided upon 4 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 2007, the Information Commissioner received 221 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 164 cases the liable body granted an applicant access to the requested information.

When resolving individual complaints, it is sometimes necessary to carry out inspection without the participation of the parties or public; the so-called 'in camera inspection' is a means by which the Information Commissioner establishes the actual state of documents at the authority's premises. 44 'in camera inspections' were carried out during 2007.
119 requests for help and various questions posed by individuals were addressed to the Information Commissioner during the course of 2007, 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.
There were no violations of procedures under the Access to Public Information Act or the Information Commissioner Act during 2007. There was, however, a perceived infringement of paragraph 6 of Article 45 of the Mass Media Act, and the perpetrator was issued a warning.

2.3. Some Significant Case Law

1.
By way of its Decision No. 021-102/2007 of 29th January 2008, the Information Commissioner granted the appeal of an applicant representing the Združenje Moč association concerning a refusal by the Social Work Centre in Maribor, and accordingly partially granted the request of the applicant. The applicant had requested statistically processed data relating to characteristics and living conditions of foster children and foster careers. In its contested refusal, the Social Work Centre claimed that it did not dispose of statistical data, and that it was not obliged to create such upon the applicant's request. In the appeal procedure, the Information Commissioner decided that if the authority disposed of data which would enable the applicant to put together or to create the requisite information, the fact that it did not dispose of the exact information which the applicant had requested did not constitute a reason for the complete rejection of the

request. The Information Commissioner thus ordered the Social Work Centre to proceed photocopies of documents or electronic records pertaining to all foster children as of 24.09.2007 from its computer application regarding foster care provision, whereby all the personal data pertaining to foster children and foster carers, which could enable the identification of any individual, should be stricken.

2.
By way of Decision No. 021-80/2007/4 of 8th September 2007, the Information Commissioner granted the appeal of an applicant pertaining to a decision by the Ministry of Justice, and consequently ordered said Ministry to hand over of a photocopy of the opinion of an expert committee as to the work of a medical doctor, whereby certain context - which would enable the identification of the individual or the applicant who was the subject of the expert opinion - had to be stricken. At the same time, the name and the surname of the court appointed expert are evident from the written record; however, in such an instance this is not an unjustified intrusion of the privacy of the expert, since it was a matter of court record and, as such, not protected personal data. It should be emphasized that the names of court experts in relation to the execution of their work are publicly accessible due to their significance. For the same reason, the committee members - court experts, who prepared the second opinion - the written record requested by the applicant - are not subject to protection as regards anonymity.

3.
Through Decision No. 021-15/2007/4 of 27th February 2007, the Information Commissioner decided as to an applicant's appeal against the Medical Chamber of Slovenia which, in the first instance, had refused access to its list of medical practitioners, namely general practitioners and family medicine specialists, who were granted concessions in 2006. In this instance the Information Commissioner founded its judgement on the provisions of the Health Services Act[10], under which health services - as a public service - are provided and undertaken within the national public health service network, which shall be carried out on the basis of a concession by public health institutions as well as other legal entities and natural persons under equal conditions. This particular case deals with a social or non-commercial public service concession. Which - owing to its nature - is undertaken in the public interest, thus demonstrated in the provision of healthcare for the citizen. There is no doubt that data on the holders of public health service concessions is public information. On the basis of its conclusions, the Information Commissioner granted the applicant's appeal and ordered the Medical Chamber of Slovenia to submit its list of medical practitioners, namely general practitioners and specialists in family medicine, who were granted a concession in 2006.

4.
Decision No. 021-67/2007/4 of 18th September 2007 was in relation to appeal against the refusal of the Medical Chamber of Slovenia to submit a list of the net salaries of its executive employees and management for March and April 2007. The Information Commissioner found in favour of the appellant, and it determined that the activities and operations of the Medical Chamber of Slovenia, as a public legal entity and - as such - a public authority, pertain to the public domain. Furthermore it is in the public interest that all medical practitioners carry out their work efficiently and competently. As, within the meaning of item 1 of the third paragraph of Article 6 of the Access to Public Information Act, the Medical Chamber of Slovenia is primarily publicly funded (the membership fee is a public contribution and funds from the state budget are also public funds), the salaries

[10] Official Gazette of RS, No. 23/2005; Health Services Act (ZZDej).

of their executives and management are accordingly a mater of public record.

5.

Decision No. 021-27/2007/8 of 10th August 2007 concerned an appeal by the limited company Hypo Leasing d.o.o. in relation to a refusal by the Ministry of Health RS. The Information Commissioner was called to decide upon the means by way of which the Ministry had partially granted the applicant's request for access to tender documentation - the Ministry had refused access to information regarding a price structure within a bid. The Information Commissioner granted the appeal and decided that the Ministry of Health had to allow access (insight) into the per unit price as well as the total price of the individual positions of various products in the documentation provided by the successful bidder, as well as indeed of all the other bidders who participated in the public procurement procedure. Supply and installation of general and office furnishings and equipment, serial general equipment, as well as general and specialist medical equipment in the completion of construction and installation works for wards D and E of the Institute of Oncology in Ljubljana. The data (price per item), stated in the bid documentation obviously does not in itself provide evidence of the bidders experience, qualification, plant, personnel, cadre, organizational capacities or the implementation procedure. Likewise such data does not disclose results as to the success of any element of the bid in relation to the individual bidder. Furthermore said documentation does not reflect the innovation, investment in development studies or human resources, merely . in this particular case - the itemised prices of various products and installations, and not the price structure which, per se, should continue to represent a business secret.

6.

By way of Decision No. 021-54/2007/4 of 21st May 2007 the Information Commissioner decided as to the appeal by the Združenje Moč association in relation to the National Association of Social Work Centres which had refused the access to the catalogue proceeded to the Ministry of Labour, Family and Social Affairs, and from which arise social welfare services as well as the tasks carried out by the social work centres, which are entrusted to them as public authorities, together with the tasks mandated them by other statutory provisions, as well as the standards and norms for the execution of individual tasks. The body refused the applicant access to this information because the said request supposedly related to data within a document which was still under preparation, and was accordingly still subject to consideration by the body; namely, premature disclosure could result in misinterpretation as to the content of the document. The Information Commissioner assessed that the sheer fact that a document might be altered on the basis of harmonization with the Ministry of Labour, Family and Social Affairs prior to its publication in the Official Gazette, did not mean that it was still under preparation. In the procedure of accepting legal norms, documents are created which are, as yet, unfinished products and are accordingly a version thereof. Each version namely represents an independent element of information which arises from the operations and field of endeavour of the authority and has been drawn up by the authority itself, or in conjunction with another body, or indeed acquired from elsewhere. On this basis the Information Commissioner granted the appeal and, by way of a decision, ordered that the requested catalogue should be handed over.

7.

Through Decision No. 21-10/2007/4 of the 18th June 2007 the Information Commissioner decided as to the appeal of an applicant in relation to the Slovenian Tax Administration,

[11] Official Gazette of RS, No. 37/2007; Economic Zones Act (ZEC)

and ordered that the latter reveal the names of 9 companies which, between 2002 and 2005, had received state aid in the form of a reduced corporation tax liability under the Economic Zones Act[11]. Access to this information was declined in the first instance consequent to it being deemed a tax secret. The Information Commissioner examined both documents from which the requested information arose, and established that they were rightly classified as confidential, as are indeed all tax related issues. The Information Commissioner then carried out a so-called public interest test and focused on the notion of 'state aid' which, by law, is defined as expenditure in the form of a tax break provision, which derives from the fact that it results in reduced revenue for the state or municipal authority, and accordingly represents a benefit or aid to the recipient. Any such tax break provides a commercial advantage in relation to those competitors who do not benefit from this scheme. There are numerous forms of state aid, of which tax relief is just one. There is no doubt that state aid in the form of tax relief under the Economic Zones Act represents disposing of assets which derive from all taxpayers, and hence, accordingly, public participation is of the essence. The public must be provided the possibility of oversight as to the rectitude of the procedure that grants tax relief, including the reduction of tax rates under the Economic Zones Act as well as the eligibility of an actual company to receive such aid from the state. Transparency as regards such information especially contributes to a higher degree of accountability of recipient enterprises towards the citizens of the Republic of Slovenia. Accordingly the Information Commissioner assessed that the public interest in such data outweighs the confidentiality of tax procedure, and thus granted the appeal of the applicant.

2.4. Overall Assessment and Recommendations re Access to Public Information

The principle of the openness as regards the public sector is also a crucial element of its fundamental function. Due to the fact that public sector authorities use budgetary and other public resources provided through taxation, and even more so because such bodies perform public duties and obligations, the public sector operating within modern democratic societies must constantly be in the eye of the public it serves, and thereby also under the scrutiny of the media. As part of this public sector, the Information Commissioner operates and performs its duties as an appellate body in a spirit of openness and transparency. The information Commissioner thus endeavours to introduce the principle of transparency into its appeal procedures pertaining to access to public information as well as the re-use of public sector information.

In the five years since implementation of the Access to Public Information Act, a shift in basic mentality should have occurred within the public sector, namely, away from the concept that the work of the public sector is carried out behind closed doors, to a more open operation and transparent function. Based on a general impression as to the response of liable authorities whose procedures have been challenged, it can be perceived that the mentality has been changed, but only slightly. The situation in 2007 was not significantly different from that in 2006; and neither did 2007 represent a milestone, but rather a consolidation of the initial level of openness and transparency in both areas of our competency, little beyond that which was achieved shortly after the Access to Public Information Act came into force.

Slovenia's public sector is well aware of the fact that it undertakes activities that are in the

public interest. Therefore it is logical that the public sector not only permits and facilitates public scrutiny, but also understands that such public surveillance and oversight is essential to its operation, and in so doing it enables the general public to participate in the exercise of power.

Such co-operation is of cardinal importance to the public sector, because its work can only be performed in an appropriate, expedient and useful way through an extant spirit of active and mutual collaboration. Some of the objective weaknesses of the public sector arise as a consequence of its exaggerated distance from the citizen; it tends to emanate the impression of a lack of organization and cohesion, and is slow in its response to new or urgent problems and challenges. All these weaknesses can be overcome by strict observance of the Access to Public Information Act and the Public Media Act, which in some cases are perceived as allies for a body which is committed to working for the public at large; on the other hand, however, it is still frequently observed that some authorities subject to the Access to Public Information Act often perceive this legislation as something which merely imposes the fact that they are obliged 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 contractors (in particular at the level of local self-governing communities). These organizations 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 are used as justification for the silence that occurs all too often in cases of addressed requests for access to public information, as well as for inaccurately and insufficiently constructed websites. Such thinking is fundamentally erroneous as it completely negates the aims and intentions of ensuring the transparent function and operation of holders of public authority. Similarly unfounded is the fear that accountable bodies occasionally express concerning the abuse or manipulation of public information by applicants. Public information is openly accessible to all, and such access is not predicated on position or citizenship. Therefore it is wrong to maintain the argument that in accessing such information the applicant acts only in their own interest, or, for example, in an entrepreneurial or commercial interest. Further to which, when providing the requisite data, a liable authority enjoys no right to either consider or judge an applicant's interest in requesting access to that information. Consequently, an applicant is not obliged to state why they are requesting information or what they need the information for.

Since the implementation of the Access to Public Information Act, the Information Commissioner has noticed that implicit refusal, namely no response or reply by a public institution or authority, has been the most frequent outcome of actual requests for public information. Indeed, the ratio between appeals against such implicit decisions and appeals against actual iterated decisions re access to public information stands at 2:1, a proportion which has remained unchanged for several years. This status quo is becoming increasingly unacceptable and unjustifiable, taking into consideration the fact that the Access to Public Information Act was adopted more than five years ago. An implicit decision - by way of either a lack of address or reply - is precluded by law. The statutory deadline for the supply of public information is comparatively long, i.e. 20 working days, and, in exceptional cases, it can be

extended by a further 30 days, which is 50 working days in together; namely, a little over two 2 calendar months. An implicit decision not to provide information is unacceptable also on the basis of the responsibility of liable bodies to actual applicants and/or the public. A person who lodges a request is entitled either to the receipt of the requisite information or a refusal which justifies and articulate the reasons for the denial of access to the information, a measure that accordingly enables examination of the decision in the appeal procedure.
During 2007 we perceived a significant increase in the charges levied for the supply of public information. According to the Access to Public Access Act, access to requested information shall be provided free of charge, while the forms of access - i.e. for the media or repro materials used to facilitate such access - photocopies, electronic transcripts etc. - may be charged in accordance with the Decree on Communication and Re-use of Public Information[12]. The framework price-list for the communication of information has been loosened by a provision which provides that the prices re material costs for services which are not stated in the pertinent paragraph, can be determined by the authority in accordance with the first paragraph of that same article; namely in a manner and amount that corresponds to the average market prices for the service of communicating information and the average cost of its own labour with a commensurate allowance for the depreciation of equipment. A precondition for the validity of any such costing is that the Ministry of Public Administration provides its consent. By way of this methodology, consent has been provided for a tariff which enable liable authorities to charge for information searches, the examination of information, its preparation for partial access, photocopying or retrieval from an information system. Such regimes cause numerous difficulties in practice. Applicants, with respect to legal regulation, anticipate relatively low costs for the access to information; however - and even though not much information may be required - charges can be disproportionably high if the communication of information requires a certain search procedure and/or examination.

An additional problem is represented by the actions of some liable authorities who, despite the relatively high costs imposed for the transfer of information, do not require an advanced payment in accordance with the Decree, but rather request that the applicant settles all costs upon the information being passed to them. As a consequence of the relatively high charges made for the retrieval of information from an information system, which is in accordance with a tariff mandated by the Ministry of Public Administration, those applicants who request access to information in an electronic format are placed at a disadvantage to those who request a paper copy, a practice which is manifestly contrary to the development of IT and information society. In endorsing a tariff, a certain degree of arbitrary action by a liable entity - which is itself not subject to appropriate limitation or control - is permitted, and costs may be charged for which said authority is not entitled. Particularly misleading in practice are the actions of those liable authorities which, via their websites or through their public information access catalogues, advertise that access is free of charge, but when an applicant requests information they are informed about the tariff and the commensurate costs which are indeed relatively high.

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 opposes the application of tariffs which enable the levy of arbitrary or uncontrolled costs. Due to inappropriate regulation of this issue, the Information Commissioner also assesses that costing and charges should also be regulated differently in the Decree on Communication and Re-use of Public Information.

[12] Decree on the communication and re-use of public information was altered (Official Gazette of RS, No.199/2007), the stated changes came into force on 8.1.2008.

On the basis of appeal proceedings, the Information Commissioner considers that both liable authorities, as well as applicants, are not adequately acquainted with the basic methods by way if which public information can be accessed. The main means of accessing public information is related to the active role of liable authorities. Access to public information would be made a lot easier if more public information was made publicly available at source, in a timely manner, and by means of digital-electronic versions in particular – i.e. without the need for specific requests or resort to access in different forms and formats. Such conduct is indeed imposed by the Access to Public Information Act. Each liable body is thus obliged to transfer as much information as possible over the Internet. Electronic provision via the Internet should particularly encompass:

1. Consolidated texts of the regulations that pertain to the sphere of work of the authority, with an Internet link to the state register of regulations;
2. Programmes, strategies, views, opinions and instructions of a general nature, which are germane to the authority's interaction with the public and legal entities, as well as for deciding upon their respective rights and obligations, together with studies and similar such documents that pertain or relate to the operations of the authority;
3. Proposals for regulations, programmes, strategies, together with similar such documents that pertain to the field of activities of the authority;
4. All publications and tendering documentation in accordance with regulations governing public procurement;
5. Complete information on the authority's activities, as well as administrative, judicial and other services;
6. All public information that has been specifically requested by applicants on three, or more, occasions.

Simultaneously liable bodies can publish other public information, which they may consider of interest or believe could be legitimately requested and accessed, via the Internet. Regular publication of information on the Internet would facilitate its more rapid and effective access by the public, thereby reducing the number of requests and complaints in relation to the Access to Public Information Act, as well as the consequent disburdening of liable authorities. Likewise, if as many openly accessible public records as possible, as well as other openly accessible forms of public information (such as publication in newsletters, the media, textbooks and other journals) were established, it would not be necessary for applicants to make specific requests. It has been noted that several liable authorities do not even have their own websites - most numerous in this category are public institutions and public service sector contractors; it is, therefore, often necessary for applicants to make special requests to be able to access any such public information. We also need to point out the inactivity of administrative inspection, which - further to the possibility of appeals to the Information Commissioner - is the body responsible for ensuring compliance with the Access to Public Information Act. Administrative inspection could initiate violation procedures against all those liable authorities who have failed to establish websites, or who haven't published a catalogue listing all the public information in their possession via their website, as prescribed by the Decree on Communication and Re-use of Public Information. In such a manner the level of knowledge of those particular legislative provisions would increase, and

should, accordingly, lead to a commensurate improvement in communication between liable authorities and the public at large.

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 the Access to Public Information 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 often considered as requests for a review and transcription of files in accordance with the procedural regulation. Regulations for the review and transcription of files demand a legal interest or reasonable benefit to be exhibited, therefore liable authorities often either erroneously ask applicants to supplement their requests for access to public information, or they wholly reject such requests because legal interest has not been shown. This interpretation is particularly common in courts of law where most requests for access to public information are rejected for the reason that a review and transcription of a judicial document is regulated by another, special, regulation (e.g. by the Criminal Procedure Act or Civil Procedure Act). It has also been noted that liable authorities are not aware of the explicit legislative provision which imposes 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 the Access to Public Information 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 often considered as requests for a review and transcription of files in accordance with the procedural regulation. Regulations for the review and transcription of files demand a legal interest or reasonable benefit to be exhibited, therefore liable bodies often either wrongly ask applicants to supplement their requests for access to public information or they wholly reject the requests because legal interest has not been shown.

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 legal aid, liable authorities should be of assistance to an unknowing applicant by searching for the type of public information that the said applicant is interested in. Even if the applicant requests extensive documentation, the liable body should not reject access to it because of the mere possibility of additional work when searching for and preparing the documentation in question. The entire communication between the 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.

Last year we noted a decrease in appeal procedures as a consequence of the re-use of public sector information. The underlying reasons for this could be diametrically opposed. An optimistic interpretation might suggest that liable authorities are maybe allowing the re-use of information to a greater extent which is the result of the successfully agreement of prices and conditions for re-use with applicants. The bleaker scenario might suggest that reasons for the decrease is for the most part a consequence of reduced interest of applicants in the re-use of information, and in particular the fact that all contracts which grant a given subject the exclusive right to the re-use of certain information, in accordance with the Access to Public Information Act, shall only be valid until the end of 2008.

Inactivity and lack of applicant interest may also underlie the decline in the number of appeals, and accordingly the Information Commissioner recommends that liable 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 use of information for the purpose of performing the primary public service of an authority, or the exchange of information between bodies responsible for the performance of public services, is not considered the re-use of information. The re-use of public information results in improved transparency and clarity as to the application and manipulation of information that commercial and non-commercial users receive from the public sector. Public sector authorities collect, produce, reproduce and disseminate a great variety of documentation in the course of performing their mandated public services, and the application of such documentation 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 than 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 the information 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 alter public information for the purposes of re-use. In effect this means that re-use for commercial purposes may be charged for; 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.

Ever since the implementation of the Access to Public Information Act, the Information Commissioner recommends that the legislation continues to comprehensively and systematically regulate the sphere of access to public information, and thus uphold the principle that by its very nature, the work of all public sector authorities is a matter of public record. The Information Commissioner has noted that those who propose different regulations - especially when it comes to key or sensitive regulations - wish to interfere in the field of access to public information, as well as remove some types and categories of information from the present range which is - in principle - openly accessible to the public.

By means of different regulations some desire to introduce a number of new absolute exemptions into the framework of openly accessible information. Additional absolute exemptions, further to those already envisaged by the Access to Public Information Act, are neither necessary nor reasonable, as it is necessary to aim to achieve uniform regulation of the access to public information in the context of legal certainty.

Two categories of exemption are namely recognized in the sphere of access to public information, absolute and relative. It is typical of absolute exemptions that the rejection of access takes place as soon as it is ascertained that such exists, whereas in cases of relative exemptions, it is typical that the body has to ascertain whether a portion of data is part of such exemptions. In order to accomplish this, a public interest test, or a test to establish the extent of harm, must necessarily be carried out; thus it can be estimated whether the interests of the public, re the publication of information, outweighs those whose vested interests are better served through continued confidentiality. If exemptions are absolute, every individual case needs to be reviewed to establish whether existing circumstances require access to certain data to be impeded. If such circumstance (exemptions) are found to exist, access is not granted, whereas in all other cases the applicant should be provided with the information. No test needs to be carried out when it comes to absolute exemptions; when it comes to relative exemptions, however, it needs to be ascertained whether such is an instance fulfils the criteria of one of the prescribed exemptions. Every individual case necessitates review, and it has to be established whether an exemption is justified or whether the right of access to public information will prevail. It is also important that the list of exemptions is as short as possible, and that individual exceptions are precisely and narrowly defined in order that they can be interpreted in a restrictive manner. As with all exemptions, those pertaining to openly accessible information need to be interpreted without much leeway for alternative understanding. The exemptions among openly accessible information are namely the category that marks the normative regulation and the practical application of the Access to Public Information Act in the most significant way. Formalized exemptions that allow little room for interpretation are of the utmost importance if society is to function in a transparent manner. Interpretation of exemptions rank among the most challenging tasks faced by competent and appellate bodies in the application of normative regulation. In light of these guidelines, the Information Commissioner does not recommend the application of such supplementary regulations.

Irrespective of the aforementioned, the 2007 Act on the Trading of Financial Instruments has been adopted, and paragraph 6 of Article 488 of this Act provides that the provisions of the Access to Public Information Act shall not apply to the disclosure of certain information. The Information Commissioner was not consulted as to the intended exclusion of access to public information, and was not included in the process of the adoption of this legislation. The situation was different concerning the Public Procurement Act, paragraph 6 of Article 22 includes a stipulation that the provisions of the act regulating access to public information do not apply to tender documentation from the time when bids are opened until the decision as to the award of a contract has been made. In the course of the legislative procedure, the Information Commissioner expressed agreement with regard to the deferral of the provisions of the Access of Public Information Act for a limited duration.

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. Whilst proscribing the regulation of personal data protection through any succession of individual ordinances, the constitutional provision anticipates and facilitates the control and oversight of personal data protection through the application of a legislative keystone, on which sector-specific law and regulation may be facilitated in accordance with Article 38 of the Constitution. 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 insurance 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 regulation of personal data protection is necessary for the sake of uniformity of principles, rules and obligations, as well as to fill the legal vacuum that would occur merely through the provision of a series of sector-specific (sectoral) laws. At the same time an all-encompassing statute renders it unnecessary for the definitions, obligations and measures regarding personal data protection, the catalogues and collections of personal data, the registration of personal data collections in connection with an individual's right to know the data that pertains to them, together with the issues regarding the supervision and the jurisdiction of the supervisory authority, to be addressed through disparate sectoral laws.

Consequently, the purpose of a systematic law is not the detailed regulation of the ways personal data may be processed in particular fields, but more an establishment of the

general rights, obligations, principles and measures that deter unconstitutional, illegal and unauthorized encroachment on the rights, the dignity and privacy of the individual in any instances where their personal data may be retained and processed. For this reason the sectoral laws must clearly define what personal data collections may be established and maintained in a particular field, as well as the elements of personal data that these individual collections may contain; the ways in which personal data is collected, possible encroachments of the individual's rights, and especially the purpose of collection and processing such personal data, should all be specifically addressed and determined through said legislation. From the perspective of the protection of the individual, it is highly advisable that sectoral law shall also define the duration which personal data may be retained (the maximum retention period).

The Personal Data Protection Act[13] 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[14].

The Personal Data Protection Act is not only a systematic law, the sixth section of the Act is also the so-called »sectoral law«. Through a very detailed determination of rights, obligations, principles and measures for data controllers, it provides a direct legal basis for personal data processing in such sectors as direct marketing, video surveillance, biometrics, the recording of entries and exits from premises, and professional supervision.

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[15]. 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 personal data. The amended legislation significantly narrowed the circle of persons liable for the entry of personal data collections into the register, since entry into the register is no longer obligatory for administrators (controllers) of personal data collections who have fewer than 50 employees; however, such regulation does not apply to those administering public sector personal data collections, a category which encompasses notaries, lawyers, detectives, bailiffs, executors of personal protection, as well as private health care and medical service providers; it also extends to administrators (controllers) of personal data whose collections include sensitive personal data together with those whose registered activities embrace the processing of sensitive personal data. Besides those exceptions stated above, controllers of personal data with fewer that 50 employees are also no longer obliged to fulfil the obligations defined in the second paragraph of Article 25 (drawing up an internal statute on procedures and measures for the protection of personal data, and the designation of persons responsible for individual collections of personal data) or the obligation prescribed by Article 26 (establishing catalogues of personal data collections) of the Personal Data Protection Act. When the original amendment was being drawn up the legislature, the Information Commissioner expressed grave concern that any such narrowing of the obligations of personal data controllers would be reflected in an intrusion into the privacy of individuals; it later cautioned that the extant obligations of data controllers did not represent an administrative hurdle that necessarily needed to be removed.

---

13 Official Gazette of RS No.86/2004m - Personal Data Protection Act (ZVOP-1).
14 Official Journal of the European Union, No. L 281, 23rd November 1995.
15 Official Gazette of RS, No. 67/2007; Personal Data Protection Act - amendments (ZVOP-1A).

The amendment to the Personal Data Protection Act, however, also brought a number of positive solutions, in particular relief for individuals to whom personal data relates, regarding the ways they may access personal data that pertains to them, namely for the purpose of exercising their constitutional right to familiarize themselves with personal data as effectively as possible (specifically determined are: shorter deadlines for access, and a provision in the regulations which introduces a general and appropriate pricelist for various written explanations or copies of data that the data controller is obliged to communicate regarding the individual's right to be familiar with their personal data; the nature of the oral explanations, confirmations and information which any individual seeking to access their own personal data is obliged to receive free of charge). The regulation on charges for the exercise of the individual's right to be familiar with personal data that pertains to them was issued in September 2007[16].

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.

3.2. Review of Activities in the Field of Personal Data Protection in 2007

During 2007, the Information Commissioner received 406 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act (ZVOP-1); namely 179 in the public sector and 227 in the private sector. There were 139 applications and complaints against public sector legal entities, 40 procedures were initiated ex officio, whereas 197 applications and complaints were made against private sector entities, and 30 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, 149 inspection procedures were initiated in relation to public sector entities and 191 in private sector entities. On the basis of Article 33 of the Inspection Act[18], 38 cautions were issued in relation to minor irregularities. 62 regulatory and administrative decisions were also handed down, whereby the liable persons were ordered to undertake measures to rectify the established irregularities. 172 inspection procedures were concluded with a decision to stay the proceedings. Within the scope of procedures pertaining to cases carried over from 2006, 22 inspections were undertaken, 19 regulatory decisions issued, and 84 decisions were made as to the termination of the inspection proceedings.

16 Official Gazette of RS No. 85/2007.
17 Official Gazette of RS No. 3/2007 – General Offences Act (ZP-1).
18 Official Gazette of RS No. 43/2007 – Inspection Act (ZIN).

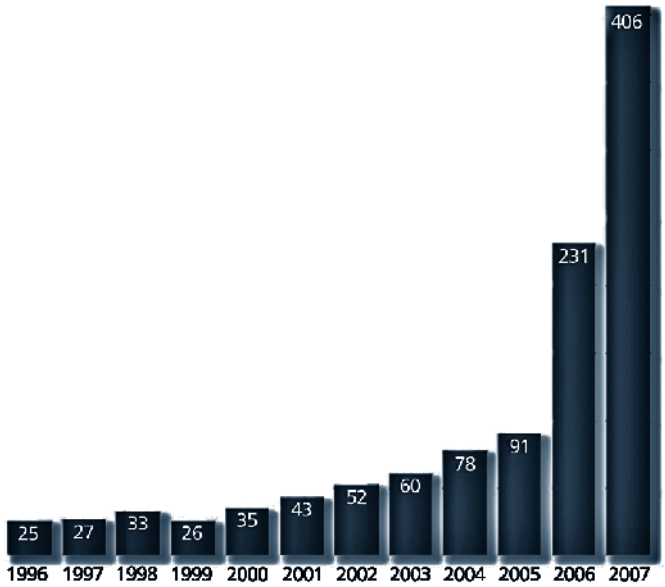


Diagram 4:

Rise in the number of applications and complaints lodged with the Information Commissioner concerning suspected violations of the Personal Data Protection Act (1996 – 2007).

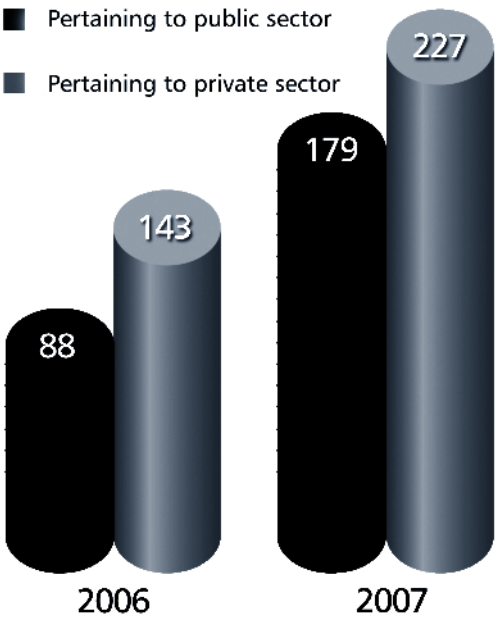


Diagram 5:

The relative number of applications and complaints made to the Information Commissioner concerning suspected violations of the Personal Data Protection Act in 2006 and 2007.

In 2007, most complaints and allegations of violations of the provisions of the Personal Data Protection Act pertained to:

- illegal collection or request for personal data (91 instances); here it should be pointed out that many of these cases involved such issues as employer's requests for data as to the state of health of employees, or the monitoring of company computers used by employees, excessive personal data collection for competition entries, or the conclusion of contracts with telecommunications service providers;
- illegal video surveillance (62), within such places as multi-storey apartment blocks and within the workplace;
- disclosure of personal data to unauthorized users by a personal data collection controller (53);
- illegal publication of personal data, for example on notice boards and in the media (48);
- insufficient personal data protection; for example, when sending information through the post (e.g. writing tax number, birth data and other such information on envelopes),

or the storage of medical records in inappropriately protected premises (29);
- misuse of personal data for the purpose of direct marketing (26),
- 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;

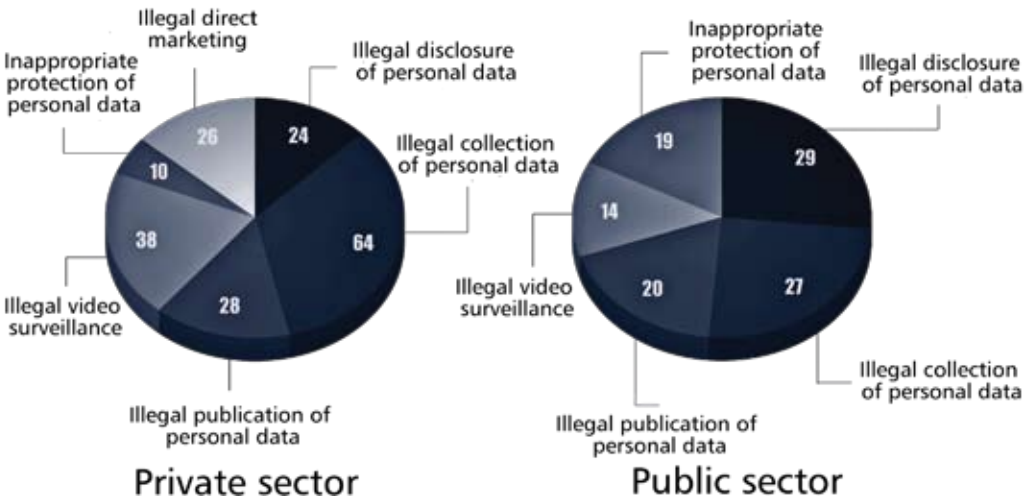


Diagram 6: The illegal processing of personal data in 2007: a comparison of the public and private sectors

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 the Act, or a mere lack of attention as regards the protection of personal data.

The most common irregularities in relation to video surveillance, established during inspections by the Information Commissioner, were as follows:
- Deficient notifications as regards the implementation of video surveillance, primarily because they did not contain the address of the person providing surveillance together with a phone number where more information could be obtained as to where and for how long the surveillance tapes would be kept. In many cases these notifications were also too small, too few or were displayed in appropriate places.
- Managers failed to provide written notification as to a 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 notify employees in writing as to video surveillance prior to its implementation. In many cases it was established that the surveillance providers failed to instigate 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.
- Most problematic in the implementation of video surveillance in multi-occupation buildings was the manner in which live recordings were simultaneously relayed to 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 more often than not personal data

contained in publicly accessible collections was being used in order to send advertising materials and other such offers. These public collections 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 more personal data than is permitted by law, further to which direct marketers often failed to inform the individuals they contacted of their right to demand - at any time and by way of a written request or indeed in any other manner - that the data controller desists from the use of their personal data in direct marketing activities.

During their inspections, Inspectors found documents containing personal data in unlocked cabinets and drawers, often in corridors; they also found unlocked or inadequately safeguarded premises and computer equipment used by data controllers. The most frequently established irregularity was insufficient traceability, or a lack of traceability, of the processing of personal data. The Information Commissioner would particularly like to point to the inadequacy of personal data protection in health care institutions.

Procedures and measures for the protection of personal data have to be commensurate with the risk represented by processing, and, as regards medical data of a personal nature, appropriate in relation to the actual circumstances of the work processes and architectural-technical solutions available at the individual facilities or service provider premises in which they are located.

As in 2006, 2007 saw the submission of many applications in relation to complaints against employers who monitored electronic mail and required medical data from their employees. 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 in accordance with the purpose 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. However, none of the above means that an employer cannot constrain the use of the company's email if it is ascertained that the employee is not using it in compliance with policy concerning the use of company assets. It is recommended that employers notify employees in advance as to how and to what extent they may use such electronic mail provision in the workplace, as well as establish rules and regulations as to when, or under what circumstances, they will monitor employees email.

There were several applications pertaining to an employer's request for access to the medical records of employees. The Information Commissioner emphasizes that employers are very restricted when it comes to 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 RS - 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. A personal physician, or another doctor or medical care professional is not at liberty to communicate data on the medical condition of a patient to an employer, unless this is expressly permitted by the patient or ordered by a court of law.

133 violation procedures (up from 41 in 2006) were initiated in 2007 as a consequence of violations of the provisions of the Personal Data Protection Act (ZVOP-1); namely: 50 procedures against public sector entities, and 83 procedures against private sector entities

As a consequence of established violations, the Information Commissioner issued:

- 42 warnings,
- 60 decisions regarding violations (46 cautions and 14 fines), and
- 11 payment orders.

In 2007, 22 offenders - legal entities, and the responsible persons of legal entities - paid fines, whereas 74 offenders who were cautioned - legal entities and the responsible persons of legal entities - paid court costs. 11 offenders (legal entities and the responsible persons of legal entities) lodged applications for judicial protection.

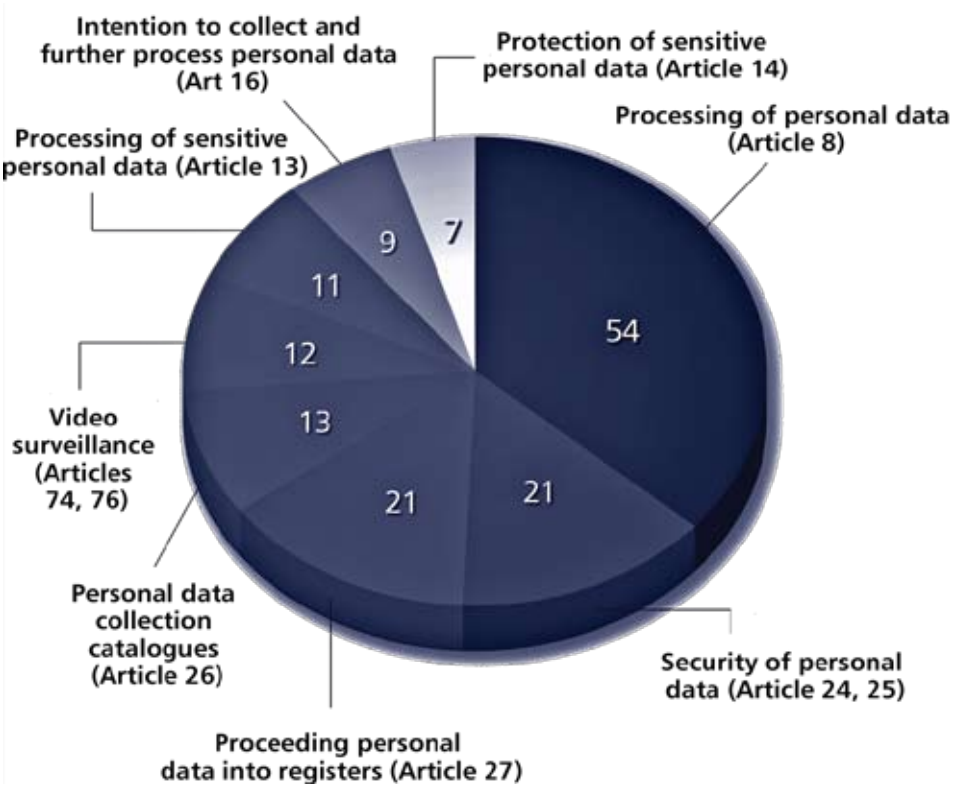


Diagram 7: The most common violations of provisions of the Personal Data Protection Act

In 2007 the Information Commissioner received 1,144 requests for written clarifications or opinions regarding specific issues, a figure which is almost double that for 2006, when the Information Commissioner received 616 such requests. The number of requests for opinions and clarifications is increasing every year, which is probably due 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 provision of written opinions and clarifications regarding the processing of personal data in individual fields represents an important part of the prevention activities of the Information Commissioner.

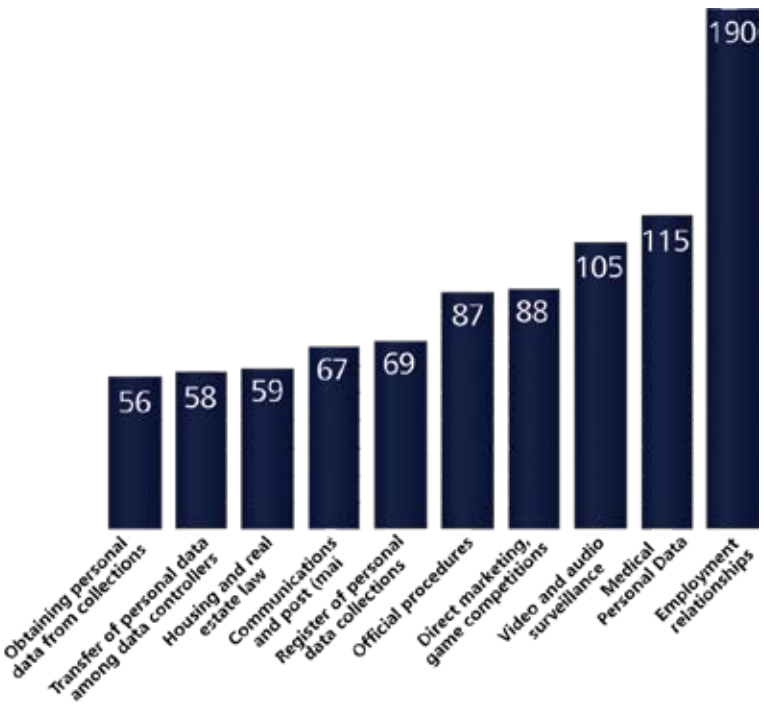


Diagram 8:

Breakdown of requests for clarifications and opinions in 2007 - according to different areas and aspects

In 2006 the Information Commissioner received 15 applications concerning the implementation of biometric measures, whereas in 2007 it received 40 applications. 35 decisions as to the admissibility of biometric measures were issued; 24 decisions vindicated the implementation of biometric measures, in one instance limited implementation was allowed, and 10 decisions proscribed the introduction of biometric measures.

Affirmative decisions were granted to those legal entities where it was established that biometric measures were vital to the performance of activities, the safety of employees and property, as well as the protection of classified information or business secrets. The Information Commissioner permitted the implementation of biometric fingerprint identification for employees entering company premises in which a server and special software, business secrets and other particularly safeguarded data were kept, as too for areas in which sensitive telecommunications equipment, which the operator is obliged to store in accordance with pertinent legislation governing the sphere of telecommunications, was in operation.

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 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, which in themselves would constitute an excessive and unnecessary violation of employee privacy, given that registering attendance can be undertaken in a less intrusive way.

Diagram 9:

Number of applications for decisions as to the admissibility of implementation of biometric measures in 2006 and 2007.

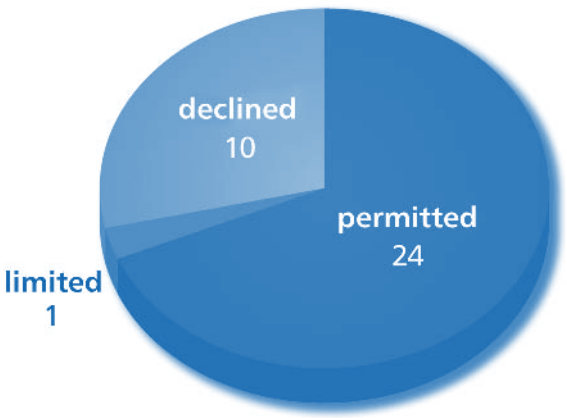


Diagram 10:

Decisions issued regarding the admissibility of implementation of biometric measures in 2007.

During 2007, the Information Commissioner received 7 applications for the export of personal data, and during the course of the year it issued two decisions regarding such matters. A company, which markets medicinal products, was allowed to export the personal data of its employees and clients to a third country, namely the USA, following the issue of decision by the Information Commissioner. This permission shall be valid for the duration of a specific contract between two legal entities, or until a new decision is issued by the Information Commissioner which may otherwise prohibit the further export of personal data. In its second decision, the Information Commissioner allowed a company which sells computer hardware, to export the personal data of both existing and potential customers, retailers, suppliers and other business partners, to Egypt, Croatia, Turkey and Taiwan, as well as its own subsidiaries and representative offices. In both decisions, the personal data that may be exported, as well as the conditions under which export is allowed, are precisely defined.

In 2007 the Information Commissioner received 12 applications for permission to merge

personal data collections; further to which, 6 decisions permitting the merging of one data collection with another were issued. The common denominator in all instances of merger was the EMŠO, Slovenia's unique personal identification number issued to all citizens. Mergers and exchanges are only permissible as regards certain types of personal data determined by law. Tax numbers, also issued to all citizens and those who work in the Republic of Slovenia, were the common element only in one instance.

During 2007, the Information Commissioner received 41 complaints as to a lack of response by an authority with regard to the right of familiarization with one's own personal data, a level significantly up on 2006, when the Information Commissioner received only 3 such complaints; 30 applications were resolved in the course of the year. Most complaints pertained to the failure of health care institutions to disclose personal data which pertained to the applicant.

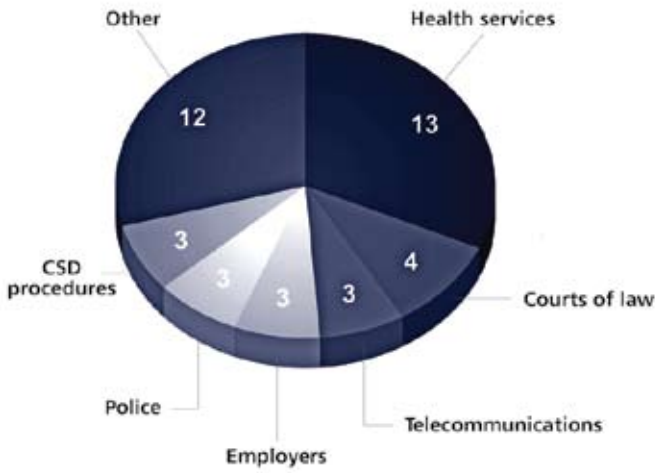


Diagram 11:

Complaints in 2007 due to lack of response with regards to requests for familiarization with one's own personal data – as per field of activities of the personal data controller

In 2007, the Information Commissioner lodged two applications for constitutional review at the Constitutional Court of the Republic of Slovenia:

- Request for the assessment of constitutionality and legality of the Health Care and Health Insurance Act[19] and the Rules on the type of data for executing supplementary health insurance[20];
- Request for an assessment as to the constitutionality and legality of the Financial Instruments Market Act[21].

The problematic provisions of the above laws are insufficient to satisfy the constitutional request for 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 regulations, which is in contravention with the Constitution RS.

The Information Commissioner received Constitutional Court Decision No. U-I-464/06-13 of 5th July 2007 regarding the Real-estate Recording Act[22]. Despite the extensive request for an assessment as to constitutionality, the Constitutional Court only partially granted

16 Official Gazette of RS, No. 72/2006 – Health Care and Health Insurance Act (ZZVZZ).
17 Official Gazette of RS, No. 7/2007; Regulations (Pravilnik).
18 Official Gazette of RS, No. 67/2007; Market in Financial Instruments Act (ZTFI)..
19 Official Gazette of RS, No. 47/2006; Real-estate Recording Act (ZEN).

the Information Commissioner's request; namely, the Court annulled that part of the Real-estate Recording Act which defines the public nature of the real estate register for natural persons (data on the owner, user, tenant, manager – their name and their unique national personal identification number (EMŠO)).

3.3. Major Violations of Personal Data Protection

1.
In March 2007, the Information Commissioner received several complaints in which applicants stated that they had received open envelopes with pre-filled-in tax returns, which enabled access to confidential data. The liable authority remedied the mistake immediately upon the receipt of the complaints, stopped the further distribution of completed tax return forms, and took steps to additionally secure all further envelopes. Due to the established irregularities pertaining to personal data protection in the distribution of completed tax returns, a violation procedure was initiated against the liable authority and their subcontractor. The violation occurred as a consequence of the failure of both the controller of the collection of personal data and its subcontractor to provide appropriate security for personal data during its transfer; i.e. they did not send the forms in envelopes which were be properly sealed. As a consequence of this failure, envelopes opened during transfer during the delivery by the postal service. The tax authority and its subcontractor had thus failed to provide adequate protection of personal data, whereby illegal processing of personal data was made possible (disclosure by transfer, reporting, spreading and otherwise making available).

2.
At the end of 2007, the Information Commissioner was examining an interesting case involving two liable entities and the suspected illegal transfer of a personal database. The database contained details of more than 140,000 individuals whose data was supposed to be transferred to the other legal entity for the purpose of sending invitations to events. Despite the fact that there had been an attempt to modify the data in such a way that the names of individuals were erased from the existing data base, the Information Commissioner's inspection proved that this was the same original database, and therewith the suspicion of illegal transfer of personal data was confirmed; accordingly, a violation procedure was initiated.

3.
Consequent to its inspection procedures, the Information Commissioner also took measures as a result of the illegal video surveillance in multi-occupation buildings. In such instances there was also the transfer of pictures, recorded as a consequence of video surveillance, to a cable-television relay. The Personal data Protection Act namely explicitly prohibits the enabling or execution of simultaneous (live) or later review (recordings) of video surveillance via an internal or public cable television channel, the Internet, or via some other means of telecommunication by way of which such footage may be transmitted. Due to the established violation of the Personal Data Protection Act, a violation procedure was initiated against the liable entity. Here it should be emphasized that video surveillance in multi-occupation buildings is, of course, possible because property and apartment owners enjoy a legitimate right to protection. Such surveillance must, however, be carried out in a justifiable manner, i.e. through the storage of recordings on hard disks or diskettes, further to which tenants must define clear rules as to who shall

have access to such recordings, and under what circumstances.

4.
The Information Commissioner inspected many health institutions during 2007, whereby special attention was paid to the protection of personal data of patients, namely those records existing in both digital (electronic) format as well as in the form of hard (paper) copies. It was established in a number of inspection procedures that sensitive personal data was being proceeded to unauthorized users; special attention was dedicated to the subject of traceability in the processing of patient data. In instances of processing sensitive data, traceability must be consistently provided in order to prevent possible disclosure or misuse (abuse) of personal data. This is achieved through appropriate safeguarding as well as the implementation of appropriate procedures and measures which provide the option of subsequent establishment as to when and by whom elements of personal data are accessed or processed. When ensuring traceability in the processing of personal data, it is not sufficient merely to ensure the subsequent establishment as to when certain data was entered into the personal data collection, or indeed when such was modified; it also has to be possible to establish subsequently when certain data was used or otherwise processed.

5.
In view of the definition of the term 'processing of personal data' from point 3 of Article 6 of the Personal Data Protection Act, there should exist - for the entire period for which the rights of the individual, re the restriction of personal data processing and transfer, are protected by law - the possibility of the subsequent establishment as to when a certain identifiable individual accessed or retrieved given elements of personal data. Procedures and measures employed for the provision of traceability depend on the manner of processing, which, in the case of personal data processed by means of automatic data processing, means that traceability must be provided by an appropriate upgrade or replacement of the computer application. By way of a regulatory decision, the latter was ordered of all healthcare institutions that did not thoroughly respect or implement the provisions of the Personal Data Protection Act.

6.
During 2007 the Information Commissioner attentively followed the situation as regards personal data processing in the media, due to the fact that the media is also obliged to respect the provisions of the Personal Data Protection Act. Further to this:

- A journalist in a daily news programme broadcast on a commercial TV station, iterated the content of a criminal complaint in a non-anonymous form. She so proceeded personal data - the surnames, names, dates of birth and unique personal identification numbers (EMŠO) - of three persons against whom charges were pending.
- A newspaper and a commercial TV station published on their official websites a photo of an ID card belonging to a person against whom an arrest warrant of had been issued. By means of this exposure they had published the following personal data: photo, name, surname, date of birth, place of birth, unique personal identification number (EMŠO), sex, ID card number, date of ID card issue, date of ID card expiry, place of ID card issue and signature.
- A newspaper published a photo of a passport of an individual who was suspected of a criminal offence, whereby the following personal data was published: photo, surname, name, citizenship, date of birth, sex, place of birth, date of passport issue, date of the expiry of the passport, passport number, unique personal identification

number (EMŠO), competent authority and signature.

- A newspaper published the content of a criminal complaint issued by the police against an individual, and in doing so disclosed the following data to the public: name, surname, date and place of birth, address, citizenship and unique personal identification number.

Upon receipt of regulatory decisions, the above perpetrators immediately removed the disputed articles and/or illegally published personal data, thus preventing further deleterious consequences. A violation of the provisions of the Personal Data Protection Act was established in all the above cases, and accordingly violation procedures were instigated against the perpetrators. Those who had infringed the Act had neither legal grounds for publishing the personal data, nor the personal permission of the individuals whose personal data they had published; at the same time the public right to know prevailed in none of the aforementioned cases. The scope of the published personal data, namely with regard to the purpose for which it was published, was inappropriate. The Information Commissioner also established that none of the individuals whose personal data had been published could be defined as public figures par excellence, so the media had no right to infringe upon their privacy, so to speak, without limitation. The extent of the personal data published went beyond that which was necessary or of interest in the public. From the perspective of public interest, namely the public's right to information and current affairs, the disclosure of limited personal data - e.g. a photo, name, surname - would have been sufficient.

3.4. Overall Assessment and Recommendations Regarding Personal Data Protection

Observations made during the performance of direct inspections in the field – which have been ongoing in Slovenia since 1995 – have revealed that this country in no way lags behind Western European standards as regards the various facets of personal data protection; indeed, Slovenia faces the same vexed issues, questions and problems as in other parts of Europe. At the same time, through the provisions of the 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 other European states. This holds particularly true in such fields as direct marketing, video surveillance, biometrics, the recording access (entry and exit) to premises, the merger of personal data collections from official records and public registers, as well as professional supervision.

Observations made during inspections reveal that the same irregularities continue to occur year after year. In the majority of cases, irregularities concerning personal data protection emanated not as a consequence of deliberate violations of the personal Data Protection Act but, above all, as a result of the poor knowledge data controllers as to the provisions of the Personal Data Act, or a mere lack of attention dedicated to the protection of personal data. Despite the latter, the Information Commissioner establishes that data controllers are becoming increasingly aware as to the importance of personal data protection, which is evident from the ongoing increase in the number of applications regarding suspected misuse of personal data, requests for opinions, clarifications and views with regard to specific issues that are raised during the course of their work and submitted to the supervisory authority.

For the purpose of raising broader awareness as to the importance of personal data protection, 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.

As a result of observations made during inspections, the Information Commissioner also concedes that it will have to pay more attention to preventive action, in the scope of which the provision of educational activities, and awareness raising among data controllers who are responsible for personal data processing, will 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 (e.g. re the provision of video surveillance, the collection of personal data in accordance with proportionality and its consequent adequate protection, as well as the familiarization of individuals with the purpose of personal data collection) 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.

More attention to the normative regulation of personal data protection will also have to be paid by the legislator as well as those responsible for drawing up legislation. The Information Commissioner has submitted a great deal of commentary on proposed legislation; the objections raised in most cases refer to insufficient definition as to the purpose, as well as disproportionate collection of personal data. 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 statutory regulations which are unconstitutional due to the very fact that they are discordant with the Constitution RS, the provisions of which request designation as to the types of personal data which shall be applicable to be 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. The legislator is thus entrusted with judgment as to the principle of proportionality, since it is the legislator who has to primarily assess what personal data shall be necessary and appropriate in meeting and fulfilling the purposes stipulated by law.

New legislation must therefore stipulate the data set and the purpose(s) for which said data may be used. If the designation of data sets are left to secondary regulation, then the doors are left open to arbitrary and unregulated assessment as to the degree of data collection by another less competent body The type of personal data to be proceeded hence always has to be stipulated by law and not secondary statute. The absence of legal grounds for the processing of personal data inevitably leads to the disproportionate - and hence illegal - processing of personal data. This is in conflict with the principle that any

invasion into the privacy of the individual must be in proportion with the value of the established legislative objective.

The degree of legitimate impingement by the legislator into the privacy and civil liberty of the citizen has to be reduced to the bare minimum that shall still enable legislative objectives to be reached. Only by way of this shall a reasonable equilibrium and balance be attained between ensuring the efficacy legislation and upholding the Constitutional rights of the individual to anonymity and privacy. In future the principle of advanced designation as to the purpose of personal data processing will also have to be observed: i.e. law will have to clearly stipulate the actual reasons behind the necessity to collect and process personal data.

The Information Commissioner also recommends that new legislation clearly stipulates the maximum period of retention for processed personal data. The Personal Data Protection Act namely only provides the controller with general guidelines as to the storage of personal data, namely for the period of time which is necessary to achieve the purpose for which the data was collected and processed. After the fulfilment of this purpose such data must be – unless otherwise provided for by law – destroyed, blocked or rendered anonymous.

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 without appropriate risk assessment as to infringements of the privacy of the individual. One such instance was the new draft law on ID cards, which entered the public domain at the end of 2007, and where the Information Commissioner perceived that there was no precise risk assessment made of provisions in relation to the protection of personal privacy, but rather than the ad-hoc adoption of draft law that invades the privacy of the individual through its consequent enabling of the merging of two databases, which were primarily established for two completely different purposes. In April 2008, by way of this new law, the legislator merged Slovenia's healthcare card with the ID card - which are two thoroughly different documents - without adequate consideration of the matter. There will now be three unique personal identifiers on the new card, two of them on the face of the card. This matter will be addressed in more detail in our 2008 annual report.

In its operations the legislator also often lags behind the extant situation, which is evident from the implementation of so-called interoperability of personal data collections. The Personal Data Protection Act namely stipulates that personal data collections from official records and public directories may only be linked if such is provided by law. Personal data controllers, who integrate two or more personal data collections that are administrated for different purposes, are obliged to inform the Information Commissioner thereof in writing. Accordingly the Information Commissioner issues permission for such integration, providing that all the legal assumptions have been fulfilled.

In practice it often happens that database integration is brought about without the provision of permission by the Information Commissioner; moreover, even without any legal provision for the accomplishment thereof. A case of such integration of personal data collections is the e-VEM project, which is basically a good, user-friendly programme; however, the legal basis for its introduction is weak and insufficiently designated by law, and indeed nonexistent as regards the integration of certain data. This is itself a case

of a large centralized collection of personal data held by the public sector which must be precisely designated. Furthermore, because of its centralization - and therewith the increased possibility of abuse - it should be subject to strict surveillance by the Information Commissioner.

It should be especially pointed out that 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 transfer via telecommunications networks.

During the course of 2007, the Information Commissioner issued several caveats as to the significance and subtlety 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 a biometric measure should first file an application for a decision by the Information Commissioner, which shall determine whether or not such introduction of biometrics is admissible and/or legal. On numerous occasions 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.

Last year, the Information Commissioner dedicated a deal of attention to the vexed question of employee expectations of privacy in the workplace. 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 out in the organization's internal statutes, accordingly acquainting employees beforehand and thus avoiding situations that would otherwise represent an inadmissible 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 admissible. Every such intrusion, defined in advance, must also, of course, be legal and acceptable in respect of constitutionally enshrined rights.

A portion of the reprimands issued by the Information Commissioner are reserved for the judiciary, which, as a consequence of the great backlog of cases - but also as a consequence of the fact that this still remains a relatively new area of law - does not resolve outstanding issues rapidly enough. Accordingly, courts are - to a great extent - disabling the work of the Information Commissioner, and this despite the fact that the provision on solving the Commissioner's cases as a matter of priority is laid down by law. In practice the Information Commissioner encounters problems emanating from a lack of efficiency and rationalization on the part of the judiciary, particularly in cases that pertain to the non co-operation of liable persons with the Information Commissioner. As the regulatory

authority, the Information Commissioner has both the right and obligation to impose fines; however, in procedures where there is resort to judicial protection by subjects upon whom a fine has been imposed, the courts are, unfortunately, far too slow in reaching their verdicts.

Trends towards the use of modern information-communication technologies (ICT), which were described in previous Information Commissioner annual reports, is continuing. Last year was marked, in particular, by the expansion of social networking sites, among the best known of which are Facebook and MySpace. Today such sites have in excess of one hundred million users, thrilled at the possibility of social networking, discovering old friends and new, exchanging information and files as well as engaging in a plethora of other networking activities. Despite the fact that from the perspective of personal data protection, this represents data processing with the personal consent of an individual, it is evident that the user awareness remains too low. According to some studies, a mere 20% of users allegedly altered their default settings (namely enabling - amongst other possibilities - how much data pertaining to the user can be seen, and by whom), regarding privacy. These are invariably set very 'openly' during registration, while the privacy policy on such sites was apparently read by a mere 0.25% of users[23] – i.e. just one user in 400! The potential consequences of reckless revelation of personal data are even more problematic when it comes to children and minors who, as a rule, are even less aware of the consequences of their actions and possible deleterious future repercussions. Theft of Internet identity on forums and websites is becoming increasingly common, whilst the bodies engaged in personal data protection are encountering an ever-larger number of such cases. Consequently, the Information Commissioner is dedicating additional attention to those issues consequential to an escalating number of questions posed by individuals who turn to the Information Commissioner for help.

Great attention has also been dedicated to the question of personal data processed in search engines, whereby the main actor in this matter has been taken over by the Article 29 Working Party. This working group, in which the Information Commissioner also participates, began drafting its opinion on this issue during 2007. An enormous amount of data is processed in the log files of the largest search engines, and this can be linked to an identifiable or designated individual. The amount and the nature of data can reflect in the creation of very detailed profiles of Internet users, which provides the temptation as to its use for a variety of purposes. Questions as to retention periods, protection, the rights of an individual to familiarization and correction, together with other classic questions pertaining to personal data protection shall be discussed in detail in the opinion, which is expected to be adopted during 2008, and will definitely attract a deal of attention from experts and broader public alike.

The Electronic Communications Act RS, which entered into force on 15th September 2007, provides the Information Commissioner with new competences and powers, namely to perform inspection control re the provisions of the Electronic Communications Act as regards the mandatory safekeeping of traffic data. Despite a contrary position being taken by the Information Commissioner regarding the safekeeping of traffic data, a maximum retention period of 24 months was adopted in the legislation. Following preliminary conclusions concerning inspection controls, it was established that there is a need for the concretization of legal provisions and the establishment of common standards which would be defined by the type and manner of use of such data.

[23] International Working Group on Data Protection in Telecommunications: Final Draft Report and Guidance on Privacy in Social Network Services – Rome Memorandum, 43rd meeting, 3–4 March 2008, Rome (Italy).

The Information Commissioner observes that new technologies are often introduced without performing appropriate preliminary risk analyses regarding privacy; indeed, such practices are particularly worrying in the public sector where a significant amount of data is being processed which can consequently be interlinked. Each technology can be used in a manner which is more or less congruous with notions of privacy; nevertheless, the Information Commissioner unfortunately all too often observes that due to ever stronger pressures regarding security, economics, practicality and short-term effects, many solutions are introduced in a manner which is not particularly in accord with the maintenance of the privacy of the individual. For this reason, more attention will have to be dedicated to privacy impact assessments, the like of which have already been established abroad, and which are primarily intended for the preliminary identification of possible invasions of privacy as well as the consequential adoption of measures that would eliminate, or at least diminish, such risks.


200GB

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 of state, the National Assembly (parliament), self-governing local communities (municipal authorities), other state institutions together with other 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 63 acts and other legislative regulations during 2007.

4.2. Relationship with the Media

Throughout the year, by way of regular and consequential co-operation with the media - by way of press conferences, press releases, statements, comments and interviews - as well as through its website, the Information Commissioner paid attention to the public character of its work and implemented measures to ensure the erudition and responsiveness of legal entities and authorities.

During 2007 the Information Commissioner renewed and redesigned its website - www.ip-rs.si. In its design, consideration was taken of the principle of transparency of activities and public awareness. As in 2006, the Information Commissioner website again received a Silver Netko Award, which was jointly presented by the Slovene Chamber of Commerce and Industry and the Ministry of Science and Technology.

Through the organization of a variety of workshops and seminars, the Information Commissioner provides for the education of liable persons and entities, further to which purpose a number of conferences, workshops and panel discussions were also organized.

On 28th January 2007, the Information Commissioner organized a public forum marking the first European Personal Data Protection Day, at which lawyers, experts from a variety of fields and well known personalities participated. Awards for good practice in the field of personal data protection in the private and public sectors were also presented on this occasion.

The Information Commissioner produced five publications during the course of 2007:

- Opinions of the Information Commissioner Concerning the Health Care Sector;
- Protecting Personal Data - a manual for personal data;
- Schengen and Your Personal Data (leaflet published in Croatian, Russian, French and English versions);
- Only You Decide;
- A Guide for the Protection of Personal Data for Parents and Teachers;
- 2006 Annual Report of the Information Commissioner.

4.3. International Co-operation

During 2007 Information Commissioner employees participated at 14 international seminars and conferences, and they presented their own contributions at six of these events.

Over the course of the year, 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 Directive 95/46/EU, the joint supervisory bodies for Europol (European law enforcement), Eurodac (European fingerprint database identifying asylum seekers) the Schengen zone and the customs union, as well as the co-ordination meetings of the European Data Protection Supervisor (EDPS) and national bodies for the protection of personal data. Within the scope of the working group in accordance with Article 29, the Information Commissioner also actively participated in the Internet and information technology sub-group.

Annual Report prepared by:

Editor:

Nataša Pirc Musar

Information Commissioner of the Republic of Slovenia

Executive Editors

Sonja Bien Karlovšek and Mojca Prelesnik

Text

Dr. Monika Benkovič Krašovec, State Supervisor for the Protection of Personal Data

Sonja Bien Karlovšek, Deputy Information Commissioner

Jože Bogataj, State Supervisor for the Protection of Personal Data

Mojca Prelesnik, Deputy Information Commissioner

Andrej Tomšič, State Supervisor for the Protection of Personal Data

Translation:

Ars Lingue, Tina Mušič, MA

Graphic design:

Klemen Mišič and Bons, d.o.o.

Ljubljana, Slovenia; July 2008

ISSN 1854-9500