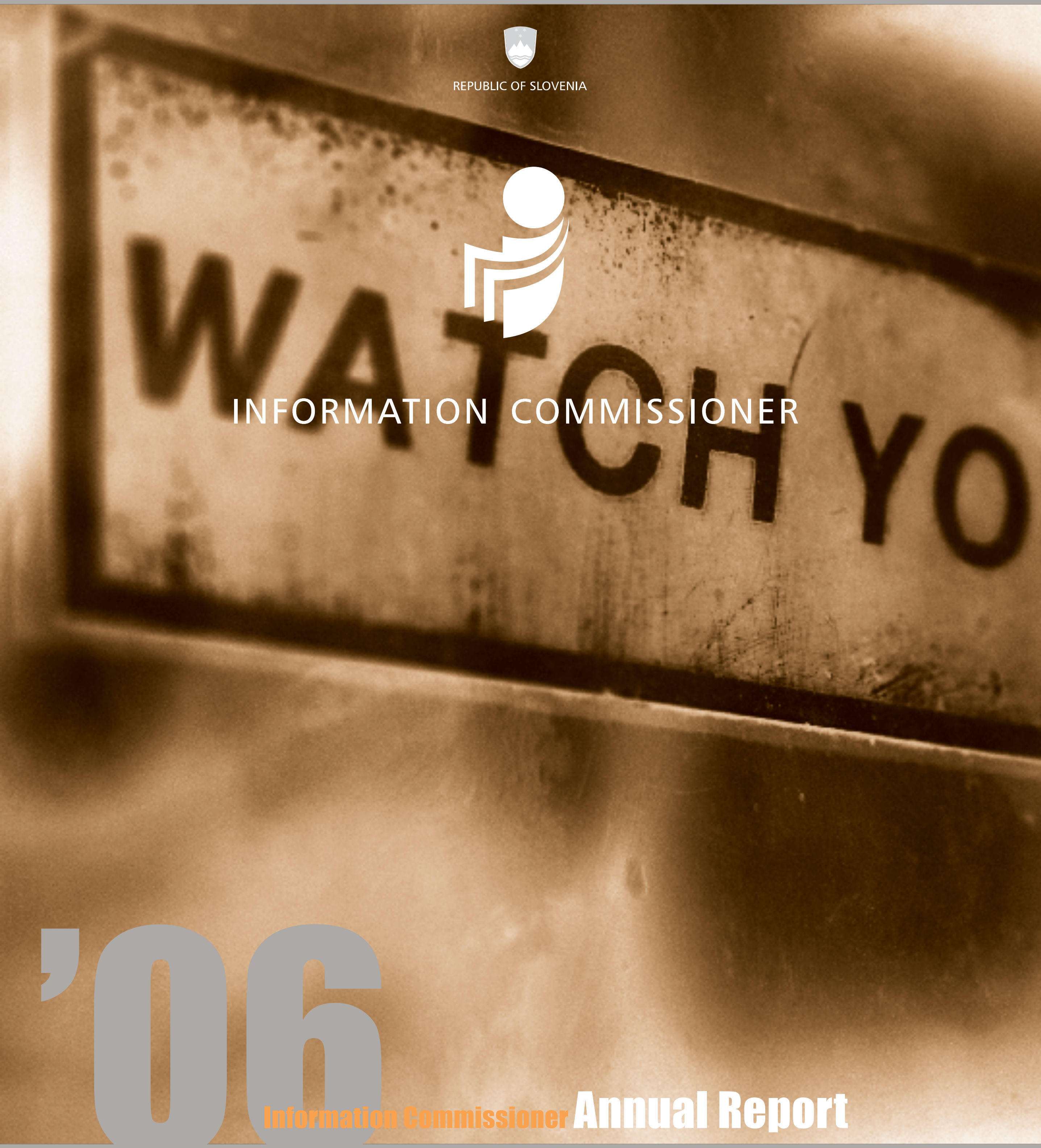
REPUBLIC OF SLOVENIA

INFORMATION COMMISSIONER



’06

Information Commissioner Annual Report 2006

REPUBLIC OF SLOVENIA

INFORMATION COMMISSIONER

’06

Information Commissioner Annual Report

2006

0 INTRODUCTION

The right of freedom of expression and the right of protection of privacy are certainly two basic principles of democracy brought into effect and enforced through the Access to Public Information Act and by the Personal Data Protection Act. The Information Commissioner is as an independent state body competent for the implementation of both acts.

Through the adoption of the Information Commissioner Act, and by expanding the jurisdiction of the former Commissioner for Access to Public Information into the field of personal data protection and thus assuring the right of information and the right of privacy of information, the work of the Information Commissioner has become more complex and varied.

The work of the Information Commissioner in relation to access to public information and the protection of personal data is for the first time presented in this its 2006 Annual Report, and as such its publication is an obligation to the National Assembly of the Republic of Slovenia as mandated by the Information Commissioner Act. This Annual Report is, of course, also intended for all those interested in the field of our endeavour.

Despite the fact that liable public sector bodies are increasingly aware of the importance of access to public information, the Information Commissioner has established that the number of complaints by applicants against a wall of silence, namely a lack of action by competent authorities, rose considerably in 2006. By taking appropriate measures the Information Commissioner has put an end to the silence of authorities, often even without resort to the issue of a binding decision, but rather through discussion of the situation or an informal warning, which is a sign of the fact that silence is not a consequence of the supreme indifference of civil servants with regard to the laws regulating access to public information, but merely a consequence of a lack of familiarity with the law. It has been noted several times that the silence has also been a consequence of temporising the access to information, which is by no means an incentive for the implementation of this fundamental human right, and is undoubtedly ethically inadmissible. The time needed for the procedure is namely of utmost importance when it comes to access to *public information; therefore it is necessary to respect the relatively long statutory time limit of twenty days, if we would like this fundamental right to be fully implemented in practice.*

An improved familiarity with the obligations of liable persons was perceived in this the third year of the enforcement of the Access to Public Information Act, while the improvement in the ability of officials working in the field of access to public information to communicate with applicants was even more appreciable. In addition to the aforementioned increase in the number of complaints as to the non-responsiveness of authorities, there was also an increase in the number of applications requesting help with interpretation of the Access to Public Information Act (with regard to formulating claims, as well as with regard to the procedure itself). The Information Commissioner has been consistent in pursuing its educational role. By taking into consideration its jurisdiction and the principle of impartiality, it has advised both authorities as well as applicants, thereby preventing the need for unnecessary appeal proceedings which might merely result from inadequate communication between applicants and liable authorities, or indeed from the insufficient familiarity of a liable individual with the particularities of the laws regulating access to public information.

In 2005 the legislator passed an amendment to the Access to Public Information Act and introduced an important novelty: a public interest test, thus making the possibility of undue obstruction of access to information less likely; said amendment also made the educational role of the Information Commissioner even more important. Progress was also evident when dealing with claims for the re-use public information, in cases where the liable authorities have the possibility to charge for re-use for profitable purposes.

In 2006 relatively few administrative disputes were raised at the Administrative Court in relation to the decisions of the Information Commissioner, which points to an improved transparency and openness of the public sector with regard to its activities and undoubtedly also to the fact that the decisions of the Information Commissioner are accepted in some way as case law by the liable authorities and applicants. Some decisions taken by the Information Commissioner as the appeal body have led to standard practice regarding the transparency of public service sector activities, including such areas as public information with regard to the salaries of civil servants, the standards and conditions applied in tendering and public contract submission procedures, as well as with regard to subsidies and the provision of other kinds of state aid, etc.

A »revolution in miniature« undoubtedly transpired in 2006 in the field of personal data protection. This law was made recognizable by liable private and public sectors entities as well as individuals, persons who are indeed the focal point of statutory implementation as well as upholding of such basic rights. The Information Commissioner conducted numerous personal data protection violation procedures during 2006, took decisions on objections made by individuals with regard to the processing of personal data, passed opinions, clarifications and views on personal data protection issues, and gave instructions and recommendations regarding personal data protection in different fields. Numerous activities were related to the upkeep of the personal data register; less than 5% of personal data controllers had been included in the register by the end of 2006; this *figure, however, was 6000 controllers more than in 2005, when only 973 personal data controllers were included. All data collection controllers are namely obliged to keep a record of collections and provide information as to such to the Information Commissioner, who in turn enters the data into the register of collections.*

Among the most important tasks of the Information Commissioner was ensuring that the provisions of the Personal Data Protection Act where adhered to. Such has been verified by the National Supervisors for personal data protection during field visits, and co-operation with ministries in the provision of personal data regulations and statute.

For the sake of better interpretation of the law in the light of innovations and development, the Information Commissioner issued a number of publications in 2006, and ensured its activities were made known throughout the year; through regular contact with the media, the provision of information on its own website and, of course, through communications with those responsible and liable, it also strived to raise awareness among legal entities, individuals and the public at large. The experts of the Information Commissioner participated in numerous educational conferences, congresses and panel discussions, and also marked the 4th International Right to Know Day. The website was completely renovated and redesigned, and new personal data protection content was included in order to improve information provision to both the expert as well as the lay public. All legal opinions (exactly 616 were issued in 2006) were published on the Internet in order to raise awareness of important issues amongst the public.

Due to the increased scope of work and due to several new fields of jurisdiction and international engagements, the number of Information Commissioner employees - and in particular the number of National Supervisors for personal data protection - increased in 2006, On 1st January 2006 the Information Commissioner had 15 employees, and this had risen to 25 by year's end. Most of the employees are lawyers, and all those working as civil servants have university degrees.

As a consequence of implementation of the Information Commissioner Act, the Information Commissioner implemented and accomplished the operational merger of two state sector organizations – the Commissioner for Access to Public Information and the former Inspectorate for Personal Data Protection.

In accordance with Article 14 of the Information Commissioner Act the Information Commissioner prepared a report about its activities during 2006, which was submitted to the National Assembly of the Republic of Slovenia in May 2007. This document contains an entire review of our work, which fills both myself and my colleagues with pride.

We will continue to make the effort, so our work can be a source of pride and assistance for the citizens of Slovenia and the country as a whole.

Nataša Pirc Musar

Information Commissioner


WATCH YOU

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, 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. Nata‘a Pirc Musar.

1.2. Jurisdiction of the Information Commissioner

The jurisdiction of the Information Commissioner is regulated by several laws.

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

- decide as to complaints against decisions by way of which an authority has rejected a request or in any other way withheld the right of access to, or re-use of, public information; and, with regard to procedures at a second instance, also in the supervision of the enforcement of the law that regulates access to public information as well as in oversight of the regulations issued on the basis of the aforementioned law;
- inspect the enforcement of law and other statute that regulate the protection and processing of personal data, the transfer of personal data from the Republic of Slovenia, as well as the performance of other duties defined by these regulations;
- decide as to complaints made by individuals when the data controller denies the request of an individual regarding their right of familiarization with the requested data, extracts, lists, access, certificates, information, clarifications, true copies or

copies under the provisions of the law that regulates the protection of personal data;

- lodge an application at the Constitutional Court of the Republic of Slovenia for a constitutional review of law, other regulations and general acts brought into force for the purpose of implementing public powers with regard to a procedure being conducted in relation to access to public information or the protection of personal data.

The Information Commissioner has jurisdiction of an appellate body under the Public Media Act[1]. 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[2].

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.[3].

In more detail, the jurisdiction of the Information Commissioner, in accordance with the Personal Data Protection Act, encompasses:

- implementation of the enforcement of inspection provisions of the Personal Data Protection Act (dealing with violations, complaints, reports and other submissions where a violation of the law is suspected);
- the imposition of the inspection measures referred to in Article 54 of the Personal Data Protection Act (prohibition of personal data processing, data anonymity, blocking, deletion or destruction of personal data when it is established that such is being processed in contravention of the law);
- imposition of other inspection measures in accordance with the Inspection Act and the General Administrative Procedure Act (point 5, first paragraph of Article 54 of the Personal Data Protection Act);
- implementation of precautionary inspection of data controllers in the public and private sectors;
- maintaining and updating the register of personal data collections and making sure that the register is updated and publicly available on the Internet (Article 28 of the Personal Data Protection Act);
- enabling access to and transcription of data from the register of personal data collections (as a rule on the same day, but within eight days at the latest (Article 29 of the Personal Data Protection Act);

1 Official Gazette of the Republic of Slovenia, No. 110/2006, official consolidated text.
2 Official Gazette of the Republic of Slovenia, No. 51/2006, official consolidated text and 117/2006-ZDavP2.
3 Official Gazette of the Republic of Slovenia, No . 86/2004 and 113/2005-ZInfP.

- conducting procedures concerning violations in the field of personal data protection (expedited procedure);
- lodging a criminal complaint and implementing procedures in accordance with the law regulating violations in the event that an inspection yields evidence of a criminal offence or a violation of the law;
- on the basis of the fourth paragraph of Article 9 and the third paragraph of Article 10 of the Personal Data Protection Act, making a decision as to the appeal of an individual in relation to personal data processing;
- issuing decisions as to the provision of adequate levels of personal data protection in third countries (Article 63 of the Personal Data Protection Act);
- conducting assessment procedures as to the adequacy of personal data protection in third countries on the basis of the findings of inspection and other information (Article 64 of the Personal Data Protection Act);
- maintaining a list of third countries regarding the fact as to whether their exists an adequate level of personal data protection, and whether, if at all, such is also fully or partially guaranteed; if it is established that a third country only partially guarantees an adequate level of personal data protection, the list also includes a specification concerning the particular fields in which adequate levels are guaranteed (Article 66 of the Personal Data Protection Act);
- conducting administrative procedures for the issue of permits for the transfer of personal data to third countries (Article 70 of the Personal Data Protection Act);
- conducting administrative procedures for the issue of permits for public records and the merger of public records when one of the data collections concerned contains sensitive personal data, or when the application of the same element (i.e. Citizen's Personal Registration Number or Tax Number) is necessary for the merger;
- conducting administrative procedures for the issue of declaratory decisions as to whether the intended implementation of biometric measures in the private sector is in accordance with the provisions of the Personal Data Protection Act;
- co-operating with state bodies, competent European Union institutions for the protection of individuals with regard to personal data processing, international institutions, foreign supervisory bodies for the protection of personal data, institutes, associations and other authorities and organizations with regard to all issues concerning the personal data protection;
- providing and publishing provisional opinions to state bodies and public authorities with regard to the conformity of provisions and regulatory proposals with laws and other statute regulating personal data;
- providing and publishing non-binding opinions with regard to the conformity of the code of professional ethics, general conditions governing business operations and the conformity of proposals with extant regulation in the field of personal data protection;
- preparing, providing and publishing non-binding instructions and recommendations with regard to personal data protection in a given field;
- publication on its website and via other pertinent means (Article 48 of the Personal Data Protection Act) of provisional opinions with regard to the conformity of proposed legislation and other regulation with extant law and existing regula-

tions regarding personal data protection, as well as applications for constitutional review;

- publication of internal journals and textbooks, court regulations and orders regarding personal data protection, as well as publication of non-binding opinions, clarifications, views and recommendations regarding personal data protection in a given field (Article 49 of the Personal Data Protection Act);
- issue of press releases regarding performed inspections and preparation of annual reports concerning its activities;
- co-operation within the context of the Working Party for personal data protection created within the EU, and which encompasses independent institutions for personal data protection in the member states, which operate on the basis of Article 29 of Directive 95/46/EC (Working Party 29);
- co-operation in joint supervisory authorities for data protection, established by the Convention on the establishment of a European Police Office (Europol); the Convention on the Use of Information Technology for Customs Purposes; the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders, and with the European Data-Protection Supervisor, established by Regulation (EC) No. 45/2001 of the European Parliament and the Council for the protection of individuals regarding personal data processing in Community institutions and bodies, together with the free movement of such data.

The Information Commissioner is also acquiring new jurisdiction. In future it will:

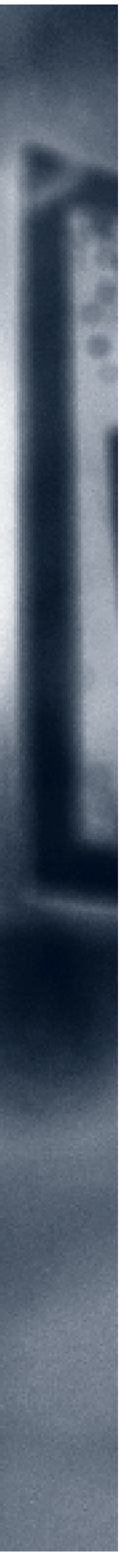
- supervise the implementation of the Schengen Agreement, Article 128 of which sets out provision for supervision by an independent institution of the monitoring of movement of personal data in the implementation of said Convention;
- be in charge of the correct implementation of the European Directive on Privacy and Electronic Communications 2002/24/ES adopted on 15th December 2005 in Brussels on the proposal of the ministers of the member states; it shall also be responsible for the prevention of abuses in the context of said directive.

1.3. Information Commissioner Organization

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

- **Information Commissioner**
  - **Cabinet of the Commissioner**
  - **Access to Public Information**
    - Complaints Resolution regarding Access to Public Information
    - Complaints Resolution regarding the Re-use of Public Information
    - Complaints Resolution regarding the Public Media Act
  - **Personal Data Protection**
    - **Inspection**
    - Maintainig Personal Data Collections Register
    - Counselling
    - Resolution of Complaints
  - **Secretariat**

Diagram 1: Information Commissioner - Organization.




WATCH YOU

2 ACTIVITIES IN THE FIELD OF ACCESS TO PUBLIC INFORMATION

2.1. Access to public information - legislation in the Republic of Slovenia

Recommendations of the Council of Europe[4] require that member states, Slovenia included, regulate the implementation of the right to access to public information through legislation, and also endorse its implementation in practice; by way of this, anybody should be able to obtain requisite information from the competent public authority.

The legislator has ensured the right of access to public information through the Constitution of the Republic of Slovenia[5]. 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**[6]. Up until then, individual provisions with regard to public information had been part of certain disparate pieces of legislation (for example the Environment Protection Act, the Protection Against Natural and Other Disasters Act); however, it has been the Access to Public Information Act that now comprehensively regulates them. 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.

The Access to Public Information Act follows the guidelines of international instruments and the guidelines prescribed by the European Union. Its aim is to ensure transparency and openness in the function and operations of public administration, as well as to ensure that everyone is entitled to public information germane to the activities of public administration bodies. The Act regulates the procedure that enables everybody free access and re-use of public information that is available to state organs, municipal authorities, public agencies, funds and other legal entities subject to public law, holders of public authorizations and providers of public services. This Act also implements the following directives of the European Community into the legal order of the Republic of Slovenia: Directive 2003/4/EC of the European Parliament and Council of 28th January 2003 on public access to environmental information and the annulment of Directive 90/313/EEC, and Directive 2003/98/EC of the European Parliament and the Council of 17th November 2003 on the re-use of public sector information.

A step forward was made in 2005 through the passing of an amendment to the Access to Public Information Act[7], 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 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 and 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.

4 Recommendation (1981) 19, and Recommendation (2002) 2.
5 Official Gazette of the Republic of Slovenia, Nos. 33/1991, 42/1997, 66/2000, 24/2003, 69/2004, 68/2006, hereinafter the Constitution of the Republic of Slovenia.
6 Official Gazette of the Republic of Slovenia, No. 24/2003.
7 Official Gazette of the Republic of Slovenia, No. 61/2005.

Restrictions on the right of access to classified information in the spheres of public safety, defence, foreign affairs, as well as intelligence and security operations are systematically regulated by the Classified Information Act[8]. Personal data is protected by the Personal Data Protection Act, however, the confidentiality of some data is also demanded by the National Statistics Act[9], the Tax Administration Act[10], the Tax Procedure Act[11], the Conservation Act[12] and the Companies Act[13].

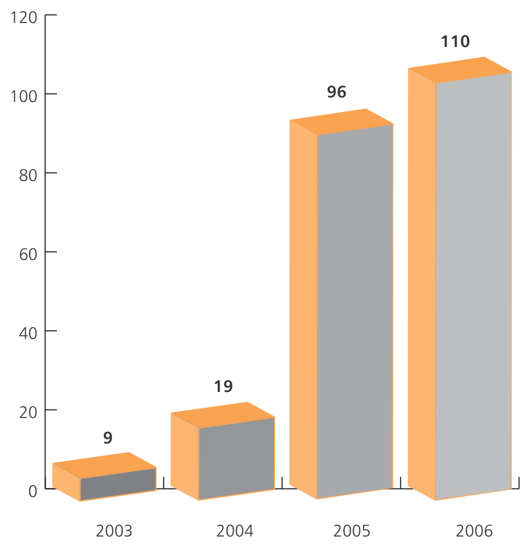
2.2. Statistical data for 2006

In 2006 **102 complaints against decisions of authorities that rejected requests for access to or the re-use of public information,** were lodged; 9 cases were carried over from 2005, and 101 complaints were resolved. The Information Commissioner received 402 complaints concerning the lack of response by authorities in 2006, and consequently it appealed to the authorities to reply with a decision as soon as possible. In 389 cases, upon receipt of an appeal, the authorities concerned approved the requests for access to the requisite information, and only 13 cases concerning a lack of response by authorities remained unresolved.

The number of decisions in the field of access to public information increases every year. **110 decisions** were handed down in 2006.

Diagram 2:

Number of decisions handed down in relation to access to public information, 2003 - 2006.



8 Official Gazette of the Republic of Slovenia, No. 135/2003, official consolidated text.
9 Official Gazette of the Republic of Slovenia, No. 45/1995, amended 9/2001.
10 Official Gazette of the Republic of Slovenia, No. 1/2007, official consolidated text.
11 Official Gazette of the Republic of Slovenia, No. 117/2006.
12 Official Gazette of the Republic of Slovenia, No. 22/2003, official consolidated text.
13 Official Gazette of the Republic of Slovenia, No. 42/2006, amended 60/2006.

In 51 cases the Information Commissioner resolved the matter in favour of the applicants, in 43 cases the complaints were rejected, in 13 cases they were partially approved; one complaint was returned to the first instance authority for reconsideration, one complaint was dismissed due to the incomplete nature of the complaint, and in one instance the decision of the first instance authority was declared void. Most of the Information Commissioner's decisions involved review as to whether the requested documents included personal data, the disclosure of which would contravene the provisions of the Personal Data Protection Act; second in quantity were decisions in which it was necessary to establish whether the liable person or authority had the document or the public information requested by the applicant in the first place. A number of decisions involved assessing whether the applicants had requested information or data that were considered business secrets according to the act regulating companies. And there were almost equal numbers of decisions which stated:

- whether the requested information was data taken from documents still in preparation and thus subject to consultation within the authority, the disclosure of which could result in a misinterpretation of their content;
- whether the requested information contained data that was considered classified on the basis of the law regulating classified data;
- 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 harm the implementation of the procedure;
- whether the authority to which the request for access to public information was addressed is liable to provide information in accordance with the Access to Public Information Act, which states in Article 1 that authorities liable for access to public information are all state bodies, local government authorities, public agencies, public funds and other entities of public law, holders of public authorizations and contracted public service providers, i.e. the entire public sector.

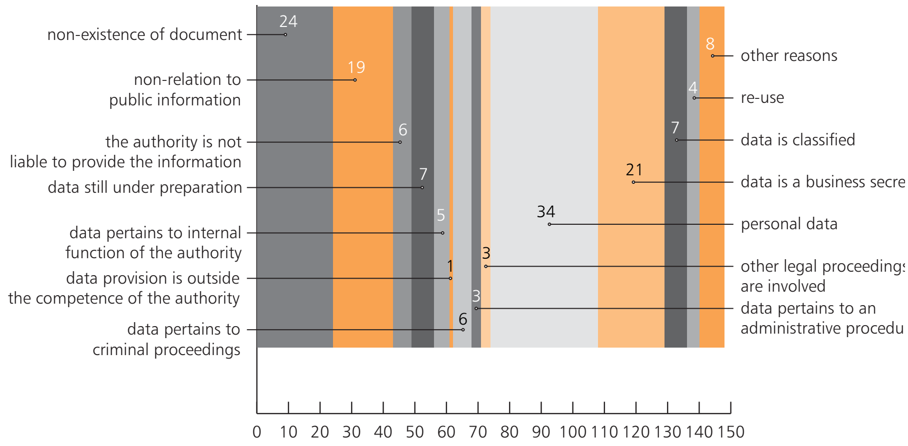


Diagram 3: Decisions taken in relation to the Access to Public Information Act with regard to various exemptions. Note that a single decision may refer to several exemptions.

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

- ministries, their constituent bodies, as well as government agencies (42),
- administrative units and municipality authorities (18),
- courts and the State Prosecutor's Office (17),
- educational institutions (6),
- health authorities (6),
- public funds, institutes, agencies and other public law entities (20),
- the Court of Auditors (1).

In 61 cases the applicants were natural persons, in 11 cases the complaints were lodged by journalists, in three cases by lawyers, and in two cases by members of the parliament. The complaints as to the lack of provision of requested information were lodged at the Information Commissioner by diverse applicants: in 12 instances by private sector legal entities, in 4 instances by municipality authorities, and in 16 instances by non-governmental organizations including associations and societies.

An appeal against the decision of the Information Commissioner is not possible; however, the initiation of an administrative dispute is envisaged under law. Fifteen such lawsuits were filed at the Administrative Court during 2006. None of these cases had been concluded by the end of 2006; the court did, however, render judgements on two decisions from previous years. The appeals were rejected in both instances.

2.3. Some significant case law

The following are some of the most challenging decisions taken in 2006, presented according to individual subject matter:

- In Case No. 021-6/2006, which dealt with an appeal made by the applicant (private sector legal entity) against a decision by the Surveying and Mapping Authority of the Republic of Slovenia, the Information Commissioner granted the appeal. The applicant requested that the body should provide information for the purposes of profitable re-use, to be exact, a digital orthophoto in the 1:5000 scale was requested, with the register of cadastral units, house numbers, and the register of geographical names (REZI 25), for the entire area of the Republic of Slovenia.
- Through decision No. 021-89/2006/7 on the appeal of the applicant (a journalist) against the decision of the Ljubljana District Court, the Information Commissioner granted the appeal and the contested decision was annulled. The body was ordered to provide the applicant with the judgement of the Ljubljana District Court within three days of the decision becoming final, whereupon all data of the claimant had to be deleted (name, surname and place of residence).
- Through decision No. 021-62/2006/2 on the appeal of the applicant, (a journalist from RTV Slovenija), against a decision by the Agency for Medicinal Products

and Medical Devices of the Republic of Slovenia, the Information Commissioner granted the appeal and the contested decision was annulled. Within three days of the decision becoming final, the body was ordered to enable the applicant access to administrative decisions it had taken during 2004 and 2005 which approved clinical trials by doctors employed at the University Hospital in Ljubljana.

- In case No. 021-77/2006/6, which dealt with an appeal by the applicant (a journalist), against a decision by Judicial Council, the Information Commissioner granted the appeal. The applicant requested the body to provide the resolution, namely the decision, which confirmed a negative assessment of the service of a serving judge.
- Decision No. 021-18/2006/8 dealt with an appeal made by the applicant (a Liberal Democrat MP), against a decision by the Ministry of the Economy. The Information Commissioner granted the appeal and the body was ordered to disclose the document entitled »Republic of Slovenia, Privatisation Group for Telekom Slovenije: Proposal for selling the state's share in Telekom Slovenije d.d., Ljubljana, December 2005« to the applicant within three days of the decision becoming final, as the document in question did not include any classified data or business secrets.
- Through decision No. 021-106/2005/5 the Information Commissioner refused the appeal made by the applicant (a journalist from the newspaper Delo), against a decision made by the Government of Slovenia. The applicant requested access to public information (a photocopy of documents), which referred to a criminal charge, filed by the police, against the chairman of the board of directors of a health insurance company, in relation to suspicion that a criminal offence had been committed, i.e. abuse of authority.
- Decision No. 021-16/2006/4 dealt with an appeal made by the applicant Amnesty International against the Government of Slovenia. The applicant approached the body with a request to provide either a digital version or a photocopy of the draught legislation (proposed law) and any existing annexes which was intended to regulate the so-called "izbrisani" problem (i.e. the predicament of erased residents who have no recognition as to nationality). The Information Commissioner granted the appeal and the body was ordered to provide the 8th December 2005 document entitled »Constitutional law proposal for amendment of the Constitution to implement the basic constitutional charter on independence and autonomy of the Republic of Slovenia.«
- In case No. 021-61/2005/7 the Information Commissioner treated an appeal made by the applicant (a journalist), against the decision of the National Examination Centre and determined that the following information is of a public nature: the percentage of candidates at individual schools that successfully passed the matura examination in the spring term, the number of students at individual schools who achieved 30 or more points in the spring term; the average number of points achieved at individual schools in the spring term; the average number of points achieved at individual schools in two selected school years in individual matura examination subjects.
- Decision No. 021-5/2006/15, taken by the Information Commissioner, dealt with an appeal made by the applicant (a national television journalist), against the lack of response by the Ljubljana University Hospital. The applicant requested access data regarding all kinds of payments (collective agreements, contracts of employment, performance allowances etc.) that some doctors at the Ljubljana University Hospital received for clinical trials carried out in 2004 and 2005. The appeal was refused as the request was deemed to be unsubstantiated.

2.4. Overall assessment and recommendations in the field of access to public information

The Information Commissioner points out that the principle of the openness of the public sector is a fundamental function of the public sector, due to the fact that the public sector operates publicly and is also responsible to the public. Since the public sector uses budgetary and other public resources provided through taxation, and even more so because it performs public duties and obligations, it is constantly in the eye of the public, and thereby also under close inspection by the media. The Information Commissioner as part of the public sector operates and performs its duties as an appeal body in the spirit of openness and transparency; procedures, and any challenges to those procedures, have to be carried out in accordance with the interests of the appellant applicant and thereby with the interests of the public at large.

The need to ensure transparent function through ensuring that the provisions of the Access to Public Information Act are implemented, should encourage the public sector to change its mentality which incorporates the idea that the work of the public sector is carried out behind closed doors. 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 already been changed slightly. The public sector is aware of the fact that it undertakes activities which are in the public interest. Therefore it is understandable that the public sector needs to not only permit and facilitate public scrutiny, but also that such public surveillance and oversight is necessary for the public sector to operate appropriately in the first place. By doing so the public sector enables the general public to participate in the exercising of power.

Public co-operation is of great importance to the public sector, because its work can only be performed in an appropriate, expedient and useful way in a spirit of active and mutual collaboration. Some of the more noticeable weaknesses of the public sector arise as a consequence of its exaggerated distance from the citizen; it emanates the impression of a lack of organization and cohesion, and it is slow in responding 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. In its work it is often reflected that those authorities liable to the Access to Public Information Act often perceive the Act as something that merely imposes the fact that they are obliged to deal with applicants, and that having to enable access to public information diverts them from their basic tasks. Such thinking is fundamentally incorrect as it completely neglects the meaning and the aims of transparent functions and operations by public authorities. Similarly unfounded is the fear that liable bodies may have that applicants could manipulate or misuse public information.

Public information is openly accessible to all, and it is tied to neither position nor citizenship. Therefore it is wrong to agree with the argument that by accessing information the applicant acts only in its own interest (for example in an entrepreneurial or commercial interest). Since the principle of free access to public information is in force, the liable authority enjoys no right to either consider or judge the applicant's interest in requesting access to certain information when providing the requisite data. This means that the applicant is not obliged to state what he or she needs the information for.

On the grounds of appeal proceedings, the Information Commissioner considers that both liable authorities as well as applicants are not adequately acquainted with the basic methods by which public information can be accessed. The main means of accessing public information is namely connected with the active role of liable persons. The access to public information would be made a lot easier if more public information were passed on to the public by the liable persons themselves, in advance and without specific requests for access in different forms (by means of digital/electronic versions in particular). Such conduct is imposed by the Access to Public Information Act. Each liable body is thus obliged to transfer as much information as possible to the Internet; and, in particular:

1. Consolidated texts of regulations relating to the sphere of work of the body, linked to the state register of regulations on the Internet;
2. Programmes, strategies, views, opinions and instructions of a general nature which is important for interaction of the body with the public and legal entities, and for deciding upon their respective rights or obligations, studies, and other similar documents relating to the sphere of operations of the body;
3. Proposals for regulations, programmes, strategies, and other similar documents pertaining to the field of work of the body;
4. All publications and tendering documentation in accordance with regulations governing public procurement;
5. Complete information on their activities and administrative, judicial and other services;
6. All public information which has been requested by applicants on three, or more, occasions.

Simultaneously liable bodies can publish other public information on the Internet, that which they consider of interest and feel could be rightfully requested and accessed. Regular publication of information on the Internet would facilitate the more effective and rapid access to public information, thereby reducing the number of requests and complaints in relation to the Access to Public Information Act, and the consequent disburdening of liable bodies. Similarly, if as many openly accessible public records as possible and other openly accessible forms of public information (publications in newsletters, media, textbooks and other publications) were established, it would not be necessary for applicants to make requests. It has been noted that several liable bodies do not even have their own websites (the most numerous of which are public institutions and public service sector contractors), therefore it is often necessary for applicants to make special requests to be able to access any such public information.

It has also been noted that liable bodies 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 bodies 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.

During appeal proceedings it has also been noted that liable bodies often fail to respect the principle of legal aid, i.e. they do not assist the unaware applicant with filing and supplementing the request in accordance with the Access to Public Information Act. Such a lack of communication often results in requests for additional documents. The extent of requested documentation is often a reason for the liable bodies to dismiss the request by invoking one of the exemptions. The Information Commissioner points out that the liable body could often establish contact with the applicant using a suitable form of communication (even an informal one) permitted by the Access to Public Information Act, and thus enable the applicant acquisition of the requested information.

Applicants commonly request extensive documentation, often only due to the lack of knowledge with regard to information available from the liable body, and thereby forming an extensive request for access. In accordance with the principle of legal aid liable bodies should be of assistance to the unknowing applicant by searching for the kind public information that 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 body should be carried out in a spirit of openness and free access to public information, rather than aiming at impeding access to such information.

The Information Commissioner also recommends that liable bodies pay more attention to the re-use of public information. The re-use of public information involves its propagation and recycling by both individuals and legal entities for both profitable and non-profitable purposes, this with the exception of the original purpose within the public duty for which the documents were prepared in the first place. The use of information for the purpose of performing the public duties of the body, or the exchange of information between bodies responsible for the performance of public duties is not considered the re-use of information. The re-use of public information results in an improved transparency and clarity of the use of information that the commercial and non-commercial users receive from the public sector. Public sector bodies collect, produce, reproduce and disseminate documents, so they can perform their mandated public duties. The use of such documents for purposes other than those for which the documents were originally intended, is considered as re-use.

The aim of re-use is to gain additional value from public information, the private sector (the applicant) should namely offer something else or different than what is being offered by the body in the performance of its public duties. The point of re-using or taking advantage of public information is to add value to such information by the applicant, and thereby perform an economic function through the right of access to public information. Such a commercial function proves its economic significance, as the re-use of information results in the foundation of a public sector information market, which is one of the key markets in the dissemination of communication technology. Commercial users in particular process this information, and through the addition of new value enrich the information, offering it back to the market. It needs to be mentioned that it is the market alone, and not legislation, that facilitates the enrichment of information by commercial users.

The public sector - i.e. every individual body - is allowed to charge for the re-use of public information in accordance with paragraph 1, of Article 34a of the Access to Public Information Act. In effect this means that re-use for commercial purposes may be charged for; however, it is not necessary to do so. It is also very important to ensure that there is no discrimination among applicants, i.e. the re-use of information is allowed to all applicants at the same price and under the same conditions. Considering the beneficial effects of re-use it would indeed make sense for the liable bodies to start promoting it. Beside which, the provision that determines certain information should be published by the liable body in advance on the Internet, must be respected. The information in question is as follows: all conditions for the re-use of information, the usual price, and the calculation basis for charging for re-use in instances of specific requests.

The Information Commissioner recommends that the Access to Public Information Act 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 bodies is a matter of public record. The Information Commissioner has noted that those who propose different regulations wish to interfere in the field of access to public information, as well as to remove some types and categories of information from the range of information that is, in principle, openly accessible to the public. By means of different regulations they wish 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 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. To do so 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 public interest 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 to access to public information will prevail. It is also important that the list of exemptions is as short as possible and that such exception are defined in such a way 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 is of the opinion that the statutory application of further formalised exceptions would be counterproductive.


WATCH YOU

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 Provision 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 provided for their collection; 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 everyone 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 the provisions of 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 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 in 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 was adopted by the National Assembly of the Republic of Slovenia on 15th July 2004 and has been in force since 1st January 2005. Adopted 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.

The enforcement of the Information Commissioner Act was indicative of the complete transposition into Slovenian legislation 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.

In addition to the Constitution of the Republic of Slovenia, the Personal Data Protection Act, the Information Commissioner Act and the detailed laws regulating the processing personal data in particular sectors, the provisions of the Convention for the Protection of Individuals regarding Automatic Personal Data Processing are also enforced. The ratified Convention of the Council of Europe, published in 1994[15], ensures respect for rights and fundamental freedoms, especially the right to privacy in instances of automatic personal data processing. Such rights also pertain to every individual on the territory of every contracting party, regardless as to their citizenship or residence.

According to Article 154 of the Penal Code[16], the misuse of personal data is a criminal offence liable to obligatory criminal proceedings. A person illegally using personal data

14 Official Journal of the European Union, No. L 281, 23rd November 1995.
15 Official Gazette of the Republic of Slovenia, No. 11/1994 – International Agreements No. 3/1994.
16 Official Gazette of the Republic of Slovenia, No. 95/2004, official consolidated text.

that may only be processed in accordance with the law and the personal consent of an individual to whom such data pertains, or a person hacking into an electronic data collection with the intention of gaining personal information for themselves or someone else, may be punished with a fine or a prison term of up to one year. A similar offence committed by an official abusing their official capacity or powers, may be punished with a prison term of up to two years.

3.2. Inspection activities during 2006

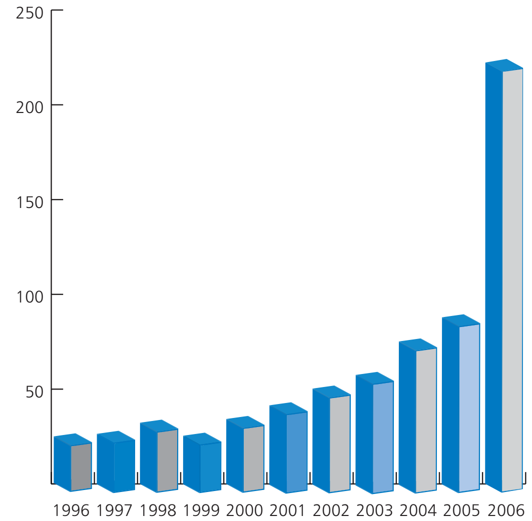
Immediate inspections pertaining to the enforcement of personal data protection regulations included:

- supervision as to the lawfulness of personal data processing;
- supervision as to the conformity of personal data protection, and the enforcement of personal data protection procedures and measures in accordance with Articles 24 and 25 of the Personal Data Protection Act;
- supervision of the enforcement of the provisions of the act regulating personal data collection catalogues, personal data collection registers, as well as records of personal data disclosure to individual users of personal data;
- supervision of the enforcement of the provisions of the act regulating personal data transfers to third countries, and personal data disclosures to foreign users of personal data.

In 2006 the Information Commissioner received **231 applications and complaints as to suspected violations of the provisions of the Personal Data Protection Act;** 88 from members of the public, and 143 from the private sector. Compared to the statistical data from previous years, the number of applications and complaints as to suspected violations of the Personal Data Protection Act are increasing.

Diagram 4:

The rise in the number of applications and complaints lodged concerning suspected violations of the Personal Data Protection Act (1996 to 2006).



Inspections instigated in 2006 as a result of **suspicion as to the misuse of personal data** pertained to:

- **Disclosure of personal data to unauthorized users** (76), i.e. enabling access to central registers by public sector administrative units. These encompass such issues as the disclosure of information pertaining to education by a faculty to a father who had lost his parenting rights; the disclosure of information about patients by health workers, despite a strict prohibition; the publication on a notice board of personal data pertaining to an employee regarding a possible disciplinary procedure; the publication of personal data in a newspaper and on the Internet; the sharing of personal data databases by student employment brokerage service providers; the disclosure of personal data on a company's clients to its business partners for the purposes of direct marketing; the disclosure of a vaccinated dog's owner's data to all veterinaries; the disclosure by a health institution of data pertaining to patients needing transport to a private ambulance service; the disclosure on notice boards of personal data pertaining to apartment owners in multi-occupation tenement buildings.
- **Illegal video surveillance** (31) at such places as a home for the aged, at the faculty pool, in the changing cubicles of stores, at children's playgrounds, in town squares, on buses, in multi-occupation buildings, as well as in bars and restaurants.
- **Collection of personal data without a legal basis or authorization** (31), including the collection of data about the state of health of employees as well as students upon matriculation; the collection of data about numbers dialled from a company phone; monitoring (performed by superiors) of emails and websites used by an employee; taking photos and filming pupils inside and outside of school without the authorization of parents; taping phone conversations without the provision of prior notice.
- **Excessive personal data collection** (28), including, order forms for school snacks which required information about the parents' employment and their personal bank account numbers; a request to send a Tax Number with the solution to a crossword puzzle; a request by a store to see a bank statement when arranging consumer credit; collection of a Citizen's Personal Registration Number and Tax Number when signing a subscription; collection of customer data when a complaint is lodged; taking photos of employees without their consent.
- **Insufficient personal data protection** (25), including, storage of medical records in unlocked cabinets in the corridors of health institutions; no provision for tractability regarding access to personal health data, unrestricted access to computer databases (unlocked offices and no password encryption for access to the database programme).
- **Sending advertising materials and direct marketing** (19) by mail (postal service), email and telephone.
- **Deficient personal data collection catalogues, and failure to transfer these to the register** (19).
- **Implementation of biometrics to monitor the attendance of employees.**

The majority of suspected misuse of personal data in the public sector involved health institutions (27), schools (31), local administrative units and municipal authorities (9), ministries (7), departments of social security (6), courts (2), and other public sector bodies (24).

The Information Commissioner received 231 applications and initiated 180 inspection procedures. In 27 cases it was clear even from the applications that the described action did not constitute a violation of the provisions of the Personal Data Protection Act. The National Supervisor explained in writing to the applicants why the described action did not constitute a violation of the provisions of the Personal Data Protection Act, and why any inspection procedure would be unreasonable. In three cases the inspection procedure was not established due to a deficient application, while in eight cases the applicants withdrew their application following a request to send more information. Four of these later merely wished for an opinion as to whether there had been a violation regarding their personal data. In one instance the violation was eliminated even before the inspection procedure had started, and in another case the inspection procedure was not initiated because there had already been an inspection procedure regarding the same violation and the decision delivered – and a request for judicial protection had also been lodged against this decision.

The Information Commissioner passed on 11 of the lodged applications to the institutions with responsibility regarding that area; 5 applications referred to violations of the provisions of Article 109 of the Electronic Communications Act regarding direct marketing via email.

In 41 cases it was established - either following an inspection by the National Supervisor or the clarifications sent by suspected offenders at the request of the National Supervisor - that there had been no violations of the Personal Data Protection Act. In these cases the National Supervisor issued a decision on cessation of the procedure on the basis of Article 28 of the Inspection Act.

On the basis of Article 33 of the Inspection Act[17], 46 cautions were issued during 2006 regarding the elimination of established minor irregularities, and these were accordingly logged in the official records. Minor irregularities that did not prompt the National Supervisor for personal data protection to issue an administrative decision, or to initiate an offence procedure, but only to issue an official caution, are those that did not involve direct interference with the rights of individuals and, furthermore, there was no intervention into the informational privacy of any individual as a consequence of the irregularity. Such minor irregularities encompass, above all, deficient data collection catalogues, insufficient or incomplete internal acts for personal data protection, insufficiently defined conditions and measures to ensure personal data protection in contract processing, minor irregularities regarding the implementation of personal data protection procedures and measures, and deficient warnings regarding video surveillance. In 7 instances pertaining to incomplete documentation, the National Supervisor appealed to the offenders to eliminate the established irregularities. When, following an official caution or an appeal, an offender eliminated the established irregularity, a decision on stopping the procedure was issued. 19 procedures concluded with the issue of a regulatory decision ordering the elimination of irregularities. Lawsuits have been filed at the Administrative Court against two decisions

The Information Commissioner resolved 113 cases during 2006, while the remaining unresolved cases were consequently transferred to 2007.

17 Official Gazette of the Republic of Slovenia, No. 56/2002, amended 26/2007.

41 violations procedures were initiated in 2006 as a consequence of violations of the provisions of the Personal Data Protection Act. The Information Commissioner reached a decision in 26 cases, while the 15 remaining (outstanding) cases were carried over to 2007. 18 cases involved private sector legal entities, while 8 cases involved public sector legal entities.

Sanctions were imposed on account of:

- deficient personal data protection (7);
- surveillance provisions violations (6);
- illegal disclosure of personal data (6);
- deficient personal data collection catalogues, and failure to transfer same to the register (5);
- direct marketing (2).

In relation to the established violations, the National Supervisor issued:

- 13 decisions regarding violations which ordered the offenders to pay a fine;
- 6 other payment orders, and
- 7 cautions.

8 offenders paid the fine, while the remaining 11 lodged applications for judicial protection.

3.2.1. Common irregularities recorded during inspections

In the majority of the cases, personal data protection violations and irregularities emanated not as a consequence of deliberate violations of the Personal Data Protection Act but, above all, as a consequence of the data controllers' poor knowledge of the provisions of the Personal Data Protection Act, or mere lack of interest in personal data protection. In some instances it was also established that the violations of the Personal Data Protection Act arose as a direct result of the negligent supervision of personal data processing by the responsible authorities. At the same time it was also established that the awareness of personal data protection, both among data controllers and among individuals, increases every year. This is corroborated by the fact that there is a constant increase in the number of applications about suspected personal data misuse, as well as in the number of requests for opinions, clarifications and recommendations submitted to the supervisory authority - on a daily basis - by data controllers and individuals.

The majority of the applications lodged by individuals in 2006 referred to the suspected disclosure of personal data to an unauthorized user. Many of the applications were unsubstantiated. The Information Commissioner stresses that Articles 8, 9 and 10 of the Personal Data Protection Act regulating general conditions of personal data processing, as well as legal frameworks for personal data processing in both the public and private sectors, must be respected when disclosing personal data. Disclosure of data is only one of the ways that personal data may be processed. When personal data from personal data collections it disclosed to other users, records are often deficient, and disclosure is commonly not recorded at all.

Article 22 of the Personal Data Protection Act determines that data controllers should record all disclosures of personal data. The aforementioned article determines that the data controller has to ensure that every disclosure of personal data can later be traced in order that it can be determined the exact nature and substance of the personal data disclosed, to whom, when and on what grounds By way of this an individual's rights against unauthorized disclosure of personal data is still possible, and hence they enjoy protection under the law. As a rule the statute of limitation set in instances of illegal disclosure of personal data is five years from when the damages were suffered, this being a general period of limitation determined by the Code of Obligations. It has been established that numerous data controllers fail to provide traceability of access to personal data collections, and that occasionally personal data disclosures to other persons are either not recorded or are recorded in a deficient manner.

The most common irregularities established during inspections related to video surveillance encompassed:

· Failure to provide the personal data collection catalogue for the surveillance system register by providers of video surveillance, and further failure to submit data from the catalogue to the Information Commissioner. According to the provisions of Article 6 of the Personal Data Protection Act, surveillance videos undoubtedly count as personal data collection when the persons in the video can be recognized.
· Deficient notifications regarding video surveillance, primarily because they did not contain the address of the person providing surveillance and 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 inappropriate places.
· Video surveillance in changing rooms and dressing rooms of shopping and sports centres.
· Failure of managers to provide a written decision regarding video surveillance, either before or after its implementation, as well as a failure to list the reasons for its implementation in any such written decision.
· Employees' non-receipt of written notification as to video surveillance prior to its implementation.
· Implementing video surveillance in communal tenements without the prior written consent of at least 70 percent of the co-owners.
· Implementation of video surveillance in a multi-occupation building in such a manner that the live recording was simultaneously relayed to a dedicated cable television channel available within the building.

Irregularities in personal data protection were often the consequence of deficient internal acts, in which organizational, logistical and technical procedures and measures for the protection of personal data should have been addressed and regulated by data controllers in accordance with the provisions of Articles 24 and 25 of the Personal Data Protection Act. Article 24 of the Personal Data Protection Act determines the requirements for personal data protection procedures as well as measures, while Article 25 determines the need for data controllers to regulate personal data protection procedures and measures in their operations, as well as oversee and ensure their implementation. With respect to this it needs to be emphasized that it is not enough for personal data protection procedures and measures to be merely regulated within the internal acts of data controllers; in addition it must be ensured that the prescribed procedures and measures are actually enforced. In order for this to happen, all employees have to be acquainted with the acts determining personal data protection procedures and measures.

In accordance with the provisions of Article 25 of the Personal Data Protection Act, data controllers must appoint individuals responsible for personal data collections, as well as identify those who may process personal data consequent to the nature of their work.

The most common instances of inadequate personal data protection pertain to:

- Inadequate storage of documentation containing personal data – documentation was stored in unlocked cabinets and drawers, often in corridors.
- Unlocked or inadequately guarded premises and computer equipment used by data controllers for storage and processing of personal data.
- Inadequate protection of computerized personal data collections – insufficient security by way of passwords for the identification and authorization of those accessing personal data.
- Traceability of personal data processing was not provided; namely, the personal data protection system did not enable determination of the time when the personal data entered personal data collection, and nor did it identify those who had accessed such data, and when.

Data controllers often overzealously collected personal data without appropriate regard to the purpose of the collection and further processing, and thus violated the principle of proportionality (Article 3 of the Personal Data Protection Act). Excessive personal data collection occurred in cases where the organizers of game competitions collected the Tax Numbers of all participants, even though only the Tax Numbers of the prizewinners would have been necessary. Excessive personal data collection also occurred in the conclusion of contracts. For example, operators offering telecommunication services collected not only Tax Numbers but also Citizen's Personal Registration Numbers, namely two identification numbers which were elements of the same kind, even though one such number would have been sufficient to identify an individual. This means that collecting two personal numbers, either of which enables the full identification of an individual, is excessive and constitutes an immoderate intervention into the privacy of an individual.

A number of irregularities were established also in the use of personal data for the purposes of direct marketing during 2006. 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, 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 utilisation 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 through a written request or in any other manner - that the data controller desists from the use of their personal data in direct marketing.

Several irregularities were also established in connection with the keeping of catalogues of personal data collections (Article 26 of the Personal Data Protection Act) and transferring data from the catalogue to the register kept by the Information Commissioner (Article 27 of the Personal Data Protection Act). There are still a great number of state institutions, local authorities, health institutions and educational establishments among the data controllers which continue to breach the aforementioned provisions. The maintenance of catalogues of personal data collections improved during 2006; however, the majority of data controllers still fail to keep their personal data catalogues up-to-date or, worst still, fail to retain such a record at all. A similar situation occurs with regard to the transfer of data from the catalogues to the Information Commissioner's register. Many data controllers still have not transferred their data from the catalogues to the register, whereas a large proportion of the data in the register is inaccurate on account of the failure of data controllers to inform the Information Commissioner as to changes of data in their collections. Due to the inaccurate and outdated data in the register, an individual's right to know is violated – when accessing the register published on the Information Commissioner website, an individual cannot determine which personal data collections are actually being kept by data controllers.

3.2.2. Major violations of personal data protection

In 2006 the Information Commissioner published several decisions that attracted a great deal of media attention. These included:

- Decision 0613-16/2006/19; on a violation by a trade company that implemented video surveillance in the changing rooms of a specialized department store, namely a breach of the provisions of Article 77 of the Personal Data Protection Act, which prohibits video surveillance in changing rooms, elevators and sanitary facilities that are not part of the workplace. Because the illegal video surveillance by the offender was a gross encroachment on the privacy and dignity of people entering the changing rooms, and also violated their constitutional rights, the Information Commissioner imposed a fine.
- Decision 0613-4/2006/19; on a violation by a newspaper publisher which, in its weekly paper, printed the names and surnames of its own employees with the highest aggregate gross earnings and basic net salaries; thus illegally using the personal data of 86 of its employees and disclosing them to the public without any legal basis or consent of the individuals consent (a breach of Article 10 of the Personal Data Protection Act). The disclosure of the data also encroached on the constitutional right of personal dignity, protection of privacy and personal rights, as well as the right to protection of their personal data. In its defence, the newspaper referred to the right to freedom of expression; however, this did not prevail in this case and the Information Commissioner imposed a fine.

- Decision 0613-1/2006/22; on a violation by a newspaper that published autopsy reports of three victims who died in front of the entrance to a discotheque. The offender also referred to the right to freedom of expression as well as public interest; however, in this instance such did not constitute a legal basis for the provision of personal data by the private sector, especially the sensitive personal data on the health and conditions of the deceased (as is especially laid down in Articles 13 and 23 of the Personal Data Protection Act). In addition, the personal data was not used in accordance with the purpose for which it had been collected. The autopsy reports were intended for use in criminal proceedings against the owner of the discotheque and in no way were they intended for publication in a newspaper. On account of the severity of the breach of the Personal Data Protection Act, the Information Commissioner imposed a fine.
- Decision 0613-75/2006; on a violation by an insurance company regarding its extremely poor protection of personal data pertaining to nearly 24,000 schoolchildren, secondary school pupils and university students. The personal data was accessible through a web application merely by supplying the number of an insurance policy. Because the data was entered into a full database in alphabetical order, an unauthorized person could - merely by guessing at a number - ascertain the personal data of all the policy holders, such as name and surname, full address, Tax Number, status of the insured person and, of course, the number of the insurance policy. It was also possible to print out the data obtained in this way. On account of a severe violation of its duty to protect personal data, a fine was imposed on the insurance company.

The Information Commissioner also examined the legality of personal data processing in the clinical testing of medicinal products, established the manner of personal data protection of patients and possible access to such data. With regard to the obtainment of the patients' prior written consents for participation in the clinical research studies, there were no irregularities, although it was established that liable persons did not create catalogues of personal data collections in relation to the clinical testing of said medicinal products; hence there was no traceability of access to the health record archives as there were no actual records of access.

3.3. Written opinions and clarifications

In 2006 the Information Commissioner received 616 requests for written clarifications or opinions regarding specific issues. The number of requests for opinions and clarifications is increasing each year (there were just 34 in 2005), which is probably due to the fact that public awareness of the Personal Data Protection Act - and the rights of individuals afforded by it - is becoming much greater.

The requests for opinions and clarifications referred to a variety of different fields; the majority pertained to the following spheres:

- Personal data in the area of labour relations (74),
- Personal data in the area of official procedures (68),

- Personal data regarding health (57),
- The register of personal data collections (45),
- Personal data and the Internet (44),
- Video surveillance (42),
- Personal data and telecommunications (37).

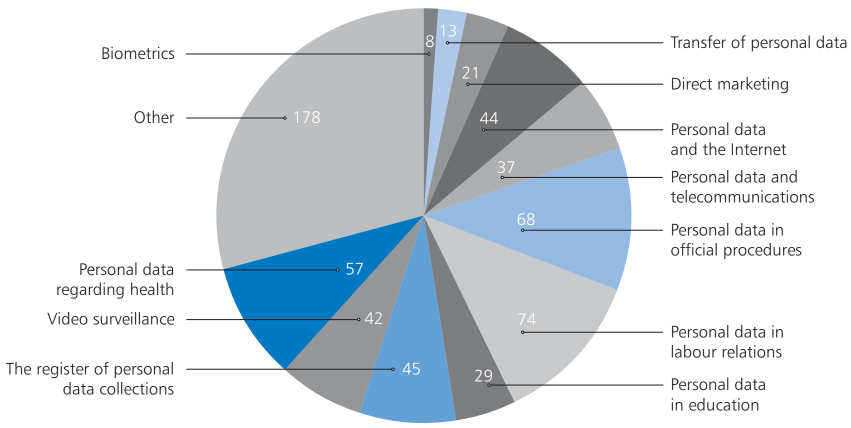


Diagram 5: Requests for the Information Commissioner's opinion during 2006, per related subject matter.

Individuals as well as public and private sector legal entities requested opinions and clarifications. Private individuals requested opinions because they believed legal entities were acting in a manner incongruous with the provisions of the Personal Data Protection Act in their processing of personal data. At the same time legal entities, from both the public and private sectors, sought advice as to how to act in specific instances, or requested interpretation of the law.

During 2006, the Information Commissioner received 268 requests from private individuals, 184 requests from public sector legal entities, and 164 requests from private companies. The majority of the individuals contacting the Information Commissioner requested an opinion or clarification concerning personal data in relation to official procedures in such fields as labour relations (34), personal data regarding health (27), personal data regarding the Internet (also 27), and video surveillance (24). The majority of public sector entities requested clarifications regarding personal data in official procedures (27), personal data regarding health (21) and personal data in the field of labour relations (18). Among the requests for opinions and clarifications submitted by private sector companies, the majority concerned the register of personal data collections (32), as well as labour relations (22) and video surveillance (12).

Issuing written opinions and clarifications regarding various aspects and applications of personal data processing, constitutes an important part of the proactive preventative actions of the Information Commissioner, and something which contributes greatly to the improvement of the situation as regards personal data protection in the Republic of Slovenia. In addition to the written opinions and clarifications, the Information

Commissioner also issued oral opinions and clarifications. Every day between 8.00 am and 4.00 pm there is always at least one employee in the office prepared to field telephone enquiries.

3.4. Admissibility in the implementation of biometric measures

In 2006 the Information Commissioner received 15 applications concerning the implementation of biometric measures; 7 applicants were private sector companies and 6 applicants were public sector legal entities. 12 decisions as to the admissibility of biometric measures were issued, two applications remained unresolved at year's end, and one application was withdrawn. In six decisions the implementation of biometric measures was permitted, in three only limited implementation was allowed, while in four applications the implementation of biometric measures was rejected outright.

Positive decisions were granted to two telecommunications operators, a hotel, an employment service, a computer company and a credit-card manufacturer, because it was established that in all these instances the implementation of biometric measures was vital for the performance of activities, the safety of employees and property, as well as the protection of classified information and business secrets. The Information Commissioner allowed the implementation of biometric fingerprint identification for employees entering protected production areas and in the personalization of credit and other cards for general use. Such was also permitted for monitoring employees entering system rooms in which classified information (business secrets) were stored (registers of card holders, of financial transactions, of credit card abuses etc.). The Information Commissioner also sanctioned the implementation of biometric measures for employees authorized to access premises with servers and computer software where, on the basis of laws regarding employment and national insurance, management is obliged to collect, process, store and further process the personal data of individuals. Positive decisions were also handed down for the implementation of biometric measures for those employees for whom management is obliged to record the working hours spent in a facility where they are exposed to ionising radiation, as well as for employees entering a premises containing telecommunication equipment which the operator is obliged to protect in accordance with pertinent legislation.

A negative decision – namely rejection of the request - was issued to the owner of a facility whose application stated that biometric measures would be implemented only for the residents of a student hall, i.e. students, and not for employees. The decision of the Information Commissioner was based on the fact that the residents of the student hall were not in an employment relationship with facility owner, meaning they were not employees. The request was thus incongruous with the provision of the Personal Data Protection Act which stipulates that the private sector can only implement biometric measures for its own employees if they have received prior written notification as to the implementation of such a measure. A similarly a negative decision was issued to a manager wishing to implement biometric measures as a means of registering members of a swimming club when entering the pool. Two negative decisions referred to the implementation of biometric measures to register private-sector employee working hours. The Information Commissioner established that the registering of attendance at a workplace is not vital for the functioning of the company, which consequently means that the implementation of biometric measures would constitute an excessive and unnecessary violation of employee privacy, given that registering attendance can be undertaken in a less intrusive way.

3.5. Ascertaining whether the levels of personal data protection in third countries is appropriate

In 2006 the Information Commissioner issued one decision regarding the export of personal data, allowing (following the issue of its decision) a Ljubljana-based legal entity functioning as a data collector to export the personal data of debit and credit card holders to a processing centre in the USA for the purpose of card processing. The exported data to be stored in the USA not longer than the duration of the card-processing contract, upon which all data would be either returned to the exporter or deleted. The company was permitted to export specifically defined personal data that pertained to individual persons, legal entities, the holders of business cards and traders, for the purpose of card processing. This permission for the export of personal data shall be valid for the duration of the contract between the American bank and the Slovenian data controller (5 years), or until a new decision is issued by the Information Commissioner which may prohibit the further export of personal data.

All other applications for personal data export referred to the countries of the former Yugoslavia, and mostly for exports to Croatia, Bosnia and Herzegovina, as well as Serbia and Montenegro. Taking into account the fact that the Information Commissioner has not issued a decision mandating that there appropriate levels of personal data protection exist in Serbia, Montenegro, Croatia and Bosnia and Herzegovina, the aforementioned countries are not included in the list of third countries which form an integral part of in Article 66 of the Personal Data Protection Act; hence personal data exports to these countries shall only be allowed if one of the conditions exhaustively determined by Article 70 of the Personal Data Protection Act is fulfilled.

Personal data exports are also possible under the provision of Point 1 of Paragraph 1 of Article 70 of the Personal Data Protection Act on the basis of laws, international agreements or ratified conventions when a certain country or its state authorities require data for the conduct of legal proceedings. Thus, data can be disclosed to Croatia on this basis and in accordance with the Act Ratifying the Agreement between the Republic of Slovenia and Republic of Croatia on Extradition, therefore such is accomplished through diplomatic channels. Data can also be disclosed on the basis of the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, ratified by Slovenia[18]; and, of course, only if the applicant country is a signatory of said Convention. A data controller may inform an individual as to a request for the disclosure of their personal data, together with the consequences of such disclosure. At the same time a data controller could request that an individual provides written consent authorizing the disclosure of their personal data if it is considered that such disclosure would be to the benefit of the individual concerned.

18 Official Gazette of the Republic of Slovenia, No. 76/2000; International Agreements No. 19/2000.

3.6. Granting permits for the merger of public records

In 2006 the Information Commissioner received 7 applications for obtaining a permit to merge personal data collections. Three applications were granted, and the citizen's ID was a common element in all these cases. Mergers and exchanges are only possible for the types of personal data determined by law.

3.7. Familiarization with your own personal data

The Information Commissioner received 3 complaints as to the lack of response by an authority with regard to the right of familiarization with one's own personal data. The complaints against lodged in relation to a rejection of leave to be familiarized with one's own personal data concerned:

1. A Police Directorate that failed to disclose to an applicant information as to whether personal data pertaining to him was being processed, a list of users of his personal data (disclosure list), as well as when, on what grounds and for what purpose, had such personal data been processed, together with the provision of all necessary explanations regarding this.
2. A health institution that failed to provide an applicant access to personal data pertaining to his deceased father, even though he proved he was the heir-at-law and that he had a legal interest in the acquisition of the requisite personal data.
3. The National Examination Centre for refusing an applicant access to exam documents pertaining to the matura examination.

In each instance the Information Commissioner requested an explanation from the liable person; the Police Directorate and the health institution consequently provided the requisite data, while the third complaint was proven to be unjustified.

3.8. Requests for assessment as to the constitutionality of laws

If, during the course of its operations and execution of procedures, an issue arises concerning constitutionality and legality, the Information Commissioner enjoys the right to lodge an application at the Constitutional Court for a constitutional review of any law, other regulation or general act which has been brought into force to implement and uphold public powers.

In 2006 the Information Commissioner lodged two applications for constitutional review at the Constitutional Court of the Republic of Slovenia; these concerned:

· Paragraphs 7 and 8 of Article 128 of the Aviation Act[19] regulating movement and restraint at public airports as well as at the premises of air traffic control services.

19 Official Gazette of the Republic of Slovenia, No. 113/2006, official consolidated text.

· Paragraph 1 of Article 96, Paragraph 2 of Article 98, Article 100, Paragraph 5 and 6 of Article 103, and Paragraph 1 of Article 114, of the Real-Estate Recording Act[20] regulating, among other matters, the recording of real estate, the real estate register, as well as the issue of data and other questions pertaining to real-estate records. In the provisions under question, the Act stipulates several items of personal data that are to be collected; however, the purpose behind their processing is inaccurate, too general and too vague.

3.9. Overall assessment and recommendations regarding personal data protection

Observations made during field visits and the performance of direct inspections - which have been practiced in Slovenia since 1995 - have revealed that this country in no way lags behind Western Europe standards as regards the various facets of personal data protection; indeed, Slovenia faces the same vexed issues, questions and problems as its European neighbours. At the same time, through the provisions of the 2003 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 of entry and exit of premises, the merger of personal data collections from official records and public registers, as well as professional supervision.

More than anyone else, it is the data collectors themselves who can contribute to improving the situation in the field of personal data protection. Data collectors are becoming increasingly aware as to the importance of personal data protection, which is evident from the constant increase in the number of requests for opinions, clarifications and views with regard to specific issues that are raised during the course of their work. However, the observations made during direct inspections reveal that the state of the majority of controllers is nevertheless not as it should be, and that almost identical irregularities are detected year after year.

Considering the ascertained situation, data controllers will need to pay more attention to ensuring up-to-date personal data collection catalogues, as well as making sure that these are included in the register of personal data collections. In view of the fact that the register of personal data collections is published on the website of the Information Commissioner, data collectors are able to check whether the data referring to their collections is current and correct, and furthermore can inform the Information Commissioner of any pertaining changes or amendments.

In future data collectors shall have to pay more attention to personal data protection, i.e. they will have to impose appropriate procedures and measures for the protection of personal data into their internal acts, inform other employees as to the existence of these acts and, most importantly, ensure the implementation of all these procedures and measures. They will also have to pay more attention to appointing persons re-

20 Official Gazette of the Republic of Slovenia, No. 47/2006.

sponsible for individual personal data collections, and to appointing persons who will - due to the nature of their work - be responsible for processing of some personal data; and in order to curtail possible misuse, the number of such people needs to remain as small as possible.

Data controllers will also have to make a lot of effort to meet all statutory requirements with regard to video surveillance. In relation to this they will have to pay special attention to the provision of appropriate notifications as well as to the issue of written ordinances on the introduction of video surveillance, which at the same time explain the reasons for such surveillance. Prior to any implementation of video surveillance, all the employees must be informed by the operator - in writing – as to the possibility of video surveillance at the premises, further to which the matter then has to be discussed with trade union representatives. As regards the video surveillance records, operators have to ensure the upkeep of the catalogue of personal data collection and pass on the data from the catalogue to the Information Commissioner, something which has - thus far - occurred only rarely.

Data controllers will also have to considerably improve the provision of information to individuals concerning the collection of personal data, as well as provide them with all the necessary information as prescribed by Article 19 of the Personal Data Protection Act. In so doing individuals too will have to be comprehensively familiarized with the purpose of personal data processing, since all too frequently the aims of such are neither clearly defined nor defined in the first place. In their collection of personal data, data controllers will have to pay more attention to the principle of proportionality. As mentioned before, it is, in most cases, inadmissible to collect two personal identification numbers (for example a citizen's personal ID number and their tax number) as just one of these two numbers suffices for the unambiguous identification of an individual. Moreover, organizers of competitions, raffles and the like, will need to cease collecting the tax numbers of all participants, as in reality they only need the tax numbers of prize winners.

More attention to the normative regulation of personal data protection will also have to be paid by the legislator and those responsible for drawing up legislative bills. When preparing statutory provisions regulating the processing of personal data in individual sectors, particular attention shall have to be paid to the principle of proportionality; i.e. sectoral law should only impose the processing of data germane to the scope of its absolute objective. The principle of advanced designation as to the purpose of personal data processing will also have to be observed; i.e. the law has to clearly stipulate the actual reason for such processing, which also needs to be constitutionally admissible. It is also recommended that any new legislation clearly stipulates the maximum retention period of processed personal data.

It has been the case in the past that the Constitutional Court of the Republic of Slovenia has annulled the data collection related provisions of legislation. Such an apparently draconian measure has transpired for several reasons: because the law stipulated excessive processing of personal data, because it did not clearly stipulate the purpose of personal data processing, or merely because the law did not clearly define what personal data is to be the subject of processing.

As a result of observations made during inspections, the Information Commissioner will also have to pay more attention to preventive action, in the scope of which the provision of educational activities, and awareness raising among data collectors responsible for personal data processing, will have to be improved. Within its jurisdiction and in co-operation with the experts, the Information Commissioner will be able to prepare and publish non-mandatory written instructions and recommendations with regard to those issues or areas that are most frequently a source of irregularities, and pass these on to the data collectors. As part of its preventive activities, the Information Commissioner will need to invigorate its preventive inspections in those areas and with those data collectors that hold several personal data collections or which process sensitive personal data. These include, in particular, data collectors in the fields of health care provision, social security and insurance operations, together with large employers, state bodies, municipal and local authorities, public service sector providers as well as other data collectors in the public sector.

In the modern era personal data processing has been inextricably linked to the application of information-communication technologies (ICT). Nowadays written databases only exist on a smaller scale, whereas the processing of larger quantities of data cannot be imagined without the application of ICT. Considering all the advantages brought into our lives by modern technology, one cannot overlook the fact that ICT also facilitates and enhances the possibilities of control and manipulation; the quantities, time, scope and duration of (personal) data processing - and the consequent possibilities for violations and abuse of extant law and the constitutional right to privacy - are all massively enhanced by ICT.

For many modern companies, personal data processing, which involves almost all activities that pertain to personal data, is today one of the keystones of business operations. Information on the behaviour of people, their status and demographic classification, their purchasing habits, their whereabouts at certain times, and the like, are of the utmost importance for the commercial sector. Metaphorically speaking, we could say that in the 21st century »data mines« are worth more than gold mines. The public sector too is aware of the importance of personal data, in particular when it comes to reinforcing the battle against terrorism; however, personal data is unfortunately too frequently collected and processed without the preparation of analyses beforehand, without a legally-defined purpose, and without due consideration as to the proportionality between safety and intrusion into the privacy of the individual.

When considering the swift development of modern information-communication technologies, nothing points to any tendency towards a decrease in the possibilities for the misuse and abuse of personal data. On the contrary, some new technologies and services, such as RFID (Radio Frequency Identification), RuBee, biometrics, technologies used for monitoring the whereabouts and movement, are a potential threat to the privacy of an individual. Some of the possibilities that seemed science fiction not so very long ago, are becoming increasingly real. Nanotechnology, RFID, biometric identification and the like, indicate tendencies for movement towards so-called object hyperlinking, where most data sources and external agents are not created by people but by the objects that belong to or are used by that individual. In an environment in which technology is omnipresent and can easily be linked via the Internet, the individual is becoming increasingly less aware of the fact as to when, where, in what ways and by whom their personal data is being processed.

With regard to these technologies, the Information Commissioner shares the views of its European counterparts (the Article 29 Working Party[21]) and by no means strives for the obstruction of entrepreneurial incentive or impediments to the development of new technologies, particularly those that could be useful for both the individual and society as a whole. However, the Information Commissioner does strive for these technologies - which are in themselves neutral - to be used in a manner that maintains the privacy of the individual. From the perspective of personal data protection, those methods of personal data processing that cause only a slight, or least, intrusion of privacy will always be favoured. It is believed that the following objectives shall contribute to the diminution of potential threats: decentralized personal data collections, improved possibilities as to the control of personal data by the individual, and intentional proportionate use of the uniform identifier.

The swift growth in the application of information-communication technologies continues to increase the possibilities of personal data abuse. Therefore the Information Commissioner pays particular attention to observation of the provisions of the Personal Data Protection Act, which regulates the protection of personal data collections, and simultaneously tries to inform the public as to the steps and measures that can be taken by an individual to protect their own personal data, particularly in relation to Internet use.

For this reason the Information Commissioner describes on its website a number of personal data abuses occurring on the Internet, and, in order to increase public awareness, also offers some recommendations for the safe use of the Internet as well as defences against potential dangers. Special attention has been paid to the so-called phishing and pharming attacks as well as spam. When it comes to phishing, skilled online fraudsters try to acquire personal data (credit card details, user names and passwords, digital certificates etc.) from people through the use of bogus websites and e-mails. Pharming attacks are more dangerous as they are more difficult to spot. The user may be totally convinced that they are on the right website, as the correct URL address of the website has been typed in; however, they have in fact been redirected to a bogus website by one of the aforementioned attacks.

In endeavouring to protect personal data online, and through striving for a safer Internet, the Information Commissioner supports the activities of SAFE-SI, the Slovenian national awareness node (http://www.safe.si/), as well as Spletno Oko (https://www.spletno-oko.si/), an online hotline which provides a means for the anonymous reporting of child pornography and hate speech on the Internet.

21 An independent Working Party established under Article 29 of EU Directive 95/46/EC which acts in an advisory capacity. It comprises the Data Protection Commissioners from the EU and a representative of the EU Commission. The Working Party seeks to harmonise the application of data protection rules throughout the EU, and publishes opinions and recommendations on various related topics; it also advises the European Commission as to the adequacy of data protection standards in non-EU countries.


WATCH YOU

4 OTHER ACTIVITIES OF THE INFORMATION COMMISSIONER

In addition to all of the aforementioned, the Information Commissioner performed also the following activities:

1. Co-operated with ministries, other authorities and organizations with regard to the preparation of legislation and other regulations determining personal data processing in particular spheres and sectors:

The Information Commissioner participated in the preparation of twenty statutes during 2006.

2. Informed, advised and educated the public as regards its activities and operations:

   The Information Commissioner organized three press conferences during 2006.

   The Information Commissioner produced eight publications during 2006.

   The Information Commissioner upgraded and revamped its website, taking into prime account the principle of transparency of operations as well as the importance of raising public awareness.

3. Educated various target groups who were directly affected by the Act on the Access to Information of Public Character and the Personal Data Protection Act in the course of their work.
4. Issued warnings to data controllers and assisted them in particular in determining adequate administrative and clerical procedures and measures for personal data protection, as well as in the preparation of appropriate internal acts.
5. Participated in seminars, conferences, consultancy sessions and meetings, both at home and abroad:

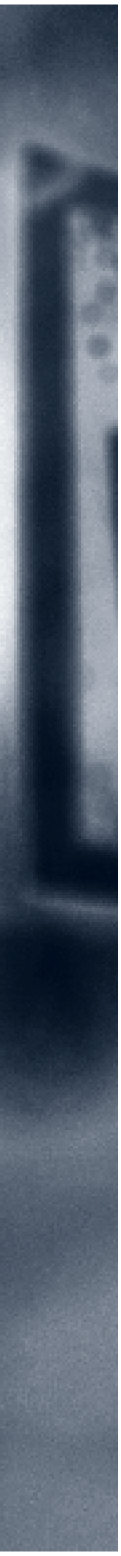
   Employees of the Information Commissioner participated in - and contributed to - 21 international seminars and during 2006.

6. Within the framework of its international co-operation activities, the Information Commissioner:

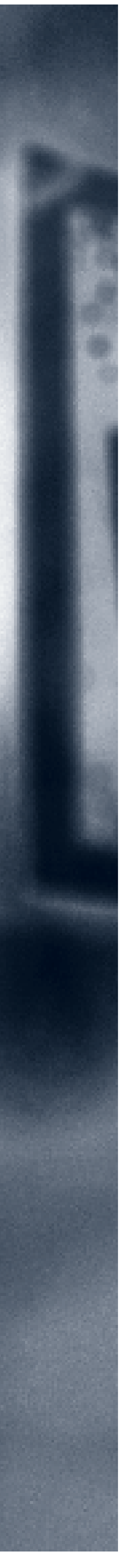
   Participated in the deliberations of the Article 29 Working Party.

   Contributed, in conjunction with other bodies of the Republic of Slovenia, in the assessment and implementation of recommendations prepared by the Schengen Evaluation Working Party.

   Participated in a joint supervisory action with the personal data protection supervisory authorities of member states, the Secretariat for Data Protection (Europol, Schengen, Customs) and the European Data Protection Supervisor (EDPS) with regard to supervising the implementation of the Eurodac system.




WATCH YOU



Annual Report prepared by:

Editor:

Nataša Pirc Musar

Information Commissioner of the Republic of Slovenia

Executive editors:

Sonja Bien Karlovšek, Deputy Information Commissioner
Mojca Prelesnik, Deputy Information Commissioner

Editor in-Chief and author:

Monika Benkovič Krašovec, Ph.D.
National Supervisor for Personal Data Protection

Authors:

Sonja Bien Karlovšek, Deputy Information Commissioner

Jože Bogataj, National Supervisor for Personal Data Protection

Urban Brulc, Researcher

Andreja Mrak, Researcher

Tanja Slak, M.A., National Supervisor for Personal Data Protection

Andrej Tomšič, M.A., Adviser

Alenka Žaucer, Adviser

Translation:

Tina Mušič

Graphic design:

Bons, d.o.o.

Printed by:

Birografika BORI d.o.o.

Published by:

Information Commissioner, August 2007

ISSN 1854-9500

INFORMATION
COMMISSIONER

REPUBLIC OF SLOVENIA