úřad pro ochranu
osobních údajů
the office for personal
data protection

ANNUAL REPORT 2003
SUMMARY

2003 was the last year of preparation for accession of the Czech Republic to the European Union. The Office for Personal Data Protection also consistently prepared for this new situation. An increased role within the Council of Europe, continued observer's status in the Brussels WP29 group, or new representation in the common supervisory body for Europol and Schengen will undoubtedly impose high requirements on the employees of the Office after accession to the European Union.

However, to obtain an equal position with the partner supervisory institutions in other EU countries and to be able to participate in the creation and development of European personal data protection, it is necessary that this part of protection of human rights and freedoms be adequately ensured in the Czech Republic: the general public in the Czech Republic must be adequately informed of their rights, the personal data controllers and processors must respect national and European legislation, and supervision of personal data processing must provide for effective and expedient remedy in cases of violation of the Personal Data Protection Act.

While the Czech Republic made another step towards harmonization with the practice in Europe during the last year, there are a number of issues that have not yet been resolved. The general public remains inadequately informed of the consequences of misuse of personal data and the controllers and processors in both the state and private sectors frequently attempt to evade, devalue or ignore the principles of protection of privacy. It will not be easy to catch up with the EU countries in the area of protection of privacy, unless the private life of individuals is considered to be an aspect that should not be devalued, particularly in the interest of a strong and viable democracy

In 2003, the Office began to contribute to improvement of personal data protection in newly established European democracies. It participated in activities of the Council of Europe concerned with the Russian Federation, Bosnia and Herzegovina, and also Cyprus. For Bosnian protectors of personal data, it organized a workshop in Prague, while in other cases, it contributed to the work of the expert group. This activity will undoubtedly be continued in the future. The Czech Republic is thus beginning to share its knowledge and experience in the area of personal data protection, which it obtained in the past from more experienced European countries.

Unfortunately, global concerns about terrorism continued in 2003. These justified concerns were accompanied by concerns related to a global epidemic – the SARS disease. These issues revealed that the world is not adequately prepared to take joint and effective measures. Similarly as the measures against terrorism, the measures that were taken against spreading of SARS were mostly isolated, uncoordinated and, in the Czech Republic, inadequately respected the rights to protection of privacy. Practically during the entire year, the European Commission held negotiations with the U.S.A. on transfer of the personal data of air passengers; a number of EU countries did not agree with the requirements of the U.S.A. Nevertheless, new terrorist threats occur and it will clearly be necessary to seek a balance between the right to privacy and risk prevention. Attention will have to be paid to this issue in the Czech Republic.

When describing the state of affairs in 2003, I cannot neglect the fact that the above-mentioned activities are now being pursued by the Office in suitable premises; however, I should also mention the issues in the area of personal data protection that were encountered by the Office:

Monitoring of persons in school facilities with the use of camera systems

Installation of camera monitoring systems was ascertained in a number of school facilities (schools, boarding houses, educational facilities). In the ensuing discussions, the representatives of school facilities were not willing to accept that this could infringe on the right of individuals to privacy. It is difficult to find accord between the requirement of schools for protection of their assets and the requirement for protecting the right of an individual to privacy.

Processing required in a democratic society

In 2003, there was an outbreak of a global epidemic of the sudden acute respiration syndrome (SARS). In the framework of preventative measures, the Ministry of Health introduced "arrival" cards, in which all passengers arriving in the Czech Republic by air were obliged to disclose information on their future whereabouts.

In this case, accord was also not found between Article 8 of the Convention for the Protection of Human Rights (the right to respect for home) and the entitlement of the state to limit this right pursuant to the Public Health Protection Act.

Distribution of commercial and advertising materials

Marketing or commercial companies still take advantage of the possibility to send their offers and advertisements until the data subject states that he no longer wants to receive advertisements (the opt-out principle). This limiting measure has not been sufficiently effective. The opposite principle – that such materials may be delivered only if the data subject so requests (the opt-in principle), as laid down in Directive 2002/58/EC, will be reflected in the legislation of the Czech Republic in 2004.

Ascertaining information on assets

A continuing issue pertains to the legally unresolved state of affairs where it is possible to ascertain the assets of natural persons and obtain access to other personal data through publicly accessible registers and lists. This issue was also evident in the area of social security, where the officials who make decisions on granting state social security benefits are not obliged to follow set procedures in ascertaining the assets of the applicants for social benefits, in order to prevent their payment to unauthorized persons.

Identity theft

Crime committed with the use of stolen personal identification data increased in 2003 both globally and in the Czech Republic. This does not always involve counterfeiting of personal documents. There are a number of cases where personal information is stolen, either from public records, by unauthorized collection of personal data obtained for various purposes or by their acquisition from databases due to their inadequate protection. In this relation, it will be necessary to reassess the approach of the Czech legislation to public registers and records. The competent state bodies must be persuaded that the structure of personal data in these public registers should be divided to a publicly accessible part and to a classified part, which would be subject to a stricter protection regime. It will also be necessary to ensure that personal data from these registers can be used only for the same purposes as those for which they were originally gathered.

Processing of biometric information

In connection with the measures adopted in the U.S.A. in the fight against global terrorism, an extensive discussion was commenced on the possible use of biometric data for personal identification. The Office for Personal Data Protection proposes that biometric personal data be classified in the Czech

Personal Data Protection Act in the category of sensitive personal data and be subjected to stricter rules for their processing. This issue will require attention during the next year when a decision will be made on issuing passports with biometric identification of their holders.

General terms and conditions of financial institutions

A relatively common unfavorable feature is that the general terms and conditions of financial institutions also contain a request for the consent of the client to acts that are not required for performance of the concluded contract. Thus, consent to the processing of personal data is often requested for marketing purposes or for transfer personal data to other entities that are not involved in performance of the concluded contract. This approach must be considered dishonest.

Legalization of data processing through the consent of the data subject

Some controllers believe that processing of personal data that is not accord with laws can be legitimized by the consent of the data subjects. Several practical issues addressed in the European Union (e.g. in transfer of personal data to the U.S.A.) document that this practice will no longer be admissible in the Czech Republic.

National health registers

Processing of personal data and sensitive data on the health condition of individuals must be regulated by law. This requirement follows both from the Personal Data Protection Act and from European regulations – Convention No. 108 and Directive 95/46/EC. A number of national health registers are operated without the relevant legal basis. A thorough review will be required from the viewpoint of the number of registers and the volume of data processed therein. It will be necessary to justify that such processing is required in democratic society in the interest of protection of the health of the general public and individuals or that it falls within the exemptions laid down for processing of sensitive data by Directive 95/46/EC (Art. 8).

Monitoring of electronic mail of employees

The issue of electronic communication will gain new dimensions next year. EU Directive 2002/58/EC on privacy in electronic communication will be reflected in the Czech legislation. The new Act will regulate a number of institutions that use electronic communication systems; this regulation will affect employees who are connected to the Internet and use electronic mail, as well as companies that use electronic communication systems for offering business and services.

RNDr. Karel Neuwirt
President

Activities of the Office in the Legislative and Legal Area

I. Position and competence of the Office

In 2003, the Personal Data Protection Act was not affected by any direct amendment and it is therefore valid as amended by laws adopted during the previous years, i.e. as amended by Acts No. 227/2000 Coll., No. 177/2001 Coll., No. 450/2001 Coll., No. 107/2002 Coll., No. 309/2002 Coll., No. 310/2002 Coll. and No. 517/2002 Coll. If the legislative process is successfully completed, the Office will be entrusted with further competence in 2004, according to amendment to Act No. 133/2000 Coll., on records of inhabitants and birth certificate numbers and on amendment to some laws, as amended, i.e. in cases involving unauthorized management of the birth certificate number or unauthorized utilization of the birth certificate number, as well as competence pursuant to the prepared Act on certain Services of Information Companies, which should at least partly deal with spamming.

II. Activities of the Office in the Legislative Area

Amendment to the Personal Data Protection Act

In accordance with the Plan of Legislative Tasks of the Government for 2003, the Office for Personal Data Protection submitted on September 30, 2003, together with the Ministry of Informatics, a draft law amending Act No. 101/2000 Coll., on personal data protection, and on amendment to some laws, as amended, for discussion by the Government.

This step concluded the stage of preparation and negotiations, which was commenced in early 2003, when a working team was established to prepare an amendment to the Act. The amendment was approved by Government Resolution No. 1086 of November 5, 2003. Immediately after completion of the governmental legislative process, the amendment was submitted for discussion by the Parliament.

The amendment to the Act was prepared in the context of the upcoming membership of the Czech Republic in the European Union and the ensuing need to harmonize the general conditions for protection of privacy in connection with personal data processing, as stipulated in the legislation of the Czech Republic, with the conditions following from international commitments of the Czech Republic in this area that are specified, in particular, in Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and in Convention No. 108 for the protection of individuals with regard to automatic processing of personal data. Therefore, it has been proposed to set the date of effect of the amendment for the date of accession of the Czech Republic to the European Union.

This intention of the Office is reflected particularly in amendment to the provisions dealing with the relation of the Personal Data Protection Act to the Community law and international treaties (Articles 1 and 27). However, some currently used terms are further specified and several new terms introduced, corresponding to Directive 95/46/EC (Article 4). This aspect is also closely related to the new regulation of the conditions for granting the consent of the data subject to personal data processing (Articles 4, 5 and 9). The provision concerning the relationship between the data controller and data subject was also amended, particularly with respect to the notification duty of the controller (Articles 11 and 12), implementation of measures on the basis of a request of the data subject (Article 21), and also modification of the condition for indemnification of the data subject in case of breach of duties by the controller or processor.

The amendment to the Act is also based on experience of the Office with application of the provisions of the Act. Although the general intention of the authors of the amendment was to provide exclusively for harmony with the Community law, the ensuing legislative process revealed some other needs, which often resulted in adopting an entirely new wording of some basic conditions for personal data processing (Article 5) and in changing the rules for use of exemptions from the Act in the procedure of the controller or processor (Articles 9 and 11).

A special chapter is devoted to amendment of penal provisions (Chapter VII). On the basis of agreement with the Ministry of Interior, the Office respects the curriculum of the concept of administrative punishment, as approved by the Government. The amendment to the penal provisions was thus supplemented on the basis of considerations contained in the material approved by the Legislative Council of the Government in August 2003.

In relation to the results of the commentary procedure, a draft amendment to Act No. 21/1992 Coll., on banks, as amended, which is concerned particularly with repeal of paragraphs 2 to 5 of Article 37, was included in the draft amendment as its Part Two. By including this part in the draft amendment, the Czech Republic will also ensure approximation of its legislation to the generally valid conditions for personal data processing in the European Union in the area of banking.

The Office had a marked contribution to the creation of legal regulations prepared by other institutions: During the year, the Office provided comments on more than 80 laws, the same number of subordinate regulations and over 30 other legislative drafts.

The entirely new Employment Act should be particularly noted among the great many legislative drafts dealt with by the Office. This regulation, which is almost a code in its nature, adopts an entirely new approach to personal data protection in the given area. It includes specific draft rules for management of personal data not only by employers, but also by state agencies that keep the relevant records. The draft Act was supplemented by the principles of personal data protection.

Important cooperation was pursued with the Ministry of Interior in preparing the draft Act amending the Act on Records of Inhabitants and Birth Certificate Numbers.

On the contrary, it is very difficult to promote the basic principles of personal data protection in relation to the Ministry of Health, which employs a more traditional, even obsolete approach to personal data protection.

The draft new Act on Health Care, which should comprehensively deal, inter alia, with the subject of legislative regulation of extensive registers and records that have been historically kept on the general public, is a good example. Ultimately, the Legislative Council of the Government proposed to return this draft to the Ministry for reworking and the issue of health registers had to be addressed in an amendment to the Act on Care for the Health of Population drafted by several MPs. The Office also provided its comments on the draft Act amending some laws in the sector of protection of public health, in relation to draft Article 79 concerning collection and processing of personal data by public health protection bodies; and also on the draft amendment to Act No. 61/1966 Coll., on certain measures against legalization of proceeds of crime and on amendment to and supplementation of some related laws, particularly in relation to the part concerning the manner and scope of identification by the obliged persons; as well as on the draft amendment to Act No. 20/1966 Coll., on care for the health of population, in relation to the part concerning data processing in case of anonymous births, according to the intentions of the parties submitting this draft. In addition to these direct activities, the Office also monitored the development of legislation in the area of state statistics and the legislative progress of preparation of the new Code of Administrative Procedure in the Chamber of Deputies.

III. Activities of the Office in the Area of Application of Law

In 2003, the Office again witnessed constant interest of the general public, as well as of individual controllers and processors of personal data, in provision of standpoints, consultations and discussions concerning application of the Personal Data Protection Act in the framework of the legislation of the Czech Republic. In the framework of these activities, the Office provided over 2000 telephonic consultations and addressed almost 1000 written petitions (and petitions sent by e-mail). It is clear from analysis of the enquiries, that the general public and the individual controllers, both in the private sector and in the governmental sector, have become sufficiently aware of the Personal Data Protection Act. However, problems arise where individual cases of processing are inadequately regulated by special laws in the area of public administration. The Czech legislation still includes great many old regulations that do not stipulate any rules for personal data processing whatsoever, although it is absolutely clear that there is a number of activities covered by these regulations, where personal data are actually processed. While the Office provides its standpoints on issues reported in these cases, these standpoints are concerned only with the competence entrusted to it, i.e. personal data processing. However, the standpoint usually describes only the approach of the Office and does not eliminate the shortcomings of the relevant regulations.

A fundamental issue in the area of public administration apparently lies both in sharing or provision of personal data from records kept by the individual agencies within their administrative agenda and in the potential for making public personal data e.g. in the framework of independent competence of municipalities or regions. The possibility or duty of municipalities or regions to provide information to the general public on their activities is an illustrative example. The regulation differs for municipalities, regions and the Capital City of Prague. This includes various forms of making public personal data by means of their presentation on the Internet, in local periodicals, etc. in cases where e.g. the resolutions of the municipal council, which also contain personal data of citizens, are made public, even if this is not permitted by the special law. The standpoints of the Office are then described as an obstacle in providing information to the general public. The Office must strictly reject these explanations: These issues arise as a direct consequence of application of special and, in this case, inconsistent legal regulations.

An entirely new area that exceeds the scope of the Personal Data Protection Act is the subject of electronic communication – in particular, spamming. Although, in these cases, electronic communication often affects privacy of individuals, there is currently no regulation that would effectively protect privacy of individuals. Therefore, in these cases, the Office is currently unable to effectively intervene, even though it has been relatively frequently enquired and asked for a standpoint on this issue, particularly during the second half of the year. This issue should be addressed through new laws in these areas that are being prepared within the competence of the Ministry of Informatics and to the preparation of which the Office has substantially contributed.

The duty of the Office to provide consultations is also largely utilized by a number of law offices, which probably use the advice and recommendations of the Office provided free-of-charge to provide their own services for the clients for consideration. This is clearly a toll for the general consulting duty of the Office, although we are convinced that the main target of the consultations should be individuals, to whose benefit and for the defense of whose fundamental right, i.e. the right to privacy, the regulation is primarily intended.

At the end of the year, the Office for Personal Data Protection was a party to several court disputes. In four cases, it acted as the plaintiff, claiming a decision, most recently before the Supreme Administrative Court, according to which it is not competent to deal with matters referred to it by the general courts for a decision in cases of protection of personal rights; a constitutional complaint from January 2002, concerning the census of

the population, houses and apartments, is still pending decision; and finally, in one case, the Supreme Administrative Court canceled a decision of the Office and returned the given matter for further examination in a case, which involved, in the opinion of the Office, personal data processing within an inappropriate scope. In this case, the Supreme Administrative Office upheld the decision of the Office for Personal Data Protection in that the controlled entity processed a number of data without authorization, nevertheless, it granted the relevant entity the right to use the birth certificate number in certain cases of processing. An action, through which a controlled entity claimed canceling of a decision on imposing a substantial fine, is also still pending decision.

Registration

Evaluation of notifications of personal data processing and requests for transfer of personal data to other countries became the task of the new Administrative Decision-Making Department in 2003. In relation to the actual assessment of individual notifications of personal data processing, two formerly separate activities of the Office concerning Article 27 of the Personal Data Protection Act (transfer of personal data to other countries) and Article 16 of the Personal Data Protection Act (notification obligation) were combined.

While the total number of submitted notifications of personal data processing remained substantially unchanged compared to the previous year, there was an increase in the number of cases where personal data were processed exclusively in connection with the transfer of personal data to other countries. With respect to new practical experience with application of statutory provisions, both on the part of the controllers and the processors and on the part of the Office, there was an increase in administrative activities in the area of the above-mentioned evaluation of personal data processing; in most cases, identical findings on specific cases of personal data processing are required for both decision-making procedures.

The current state of affairs is documented by the following surveys that indicate the number of proceedings suspended for the reason of incomplete or unclear information provided by the notifier; in these cases, the Office had to submit a request for supplementing the original petition.

For a majority of controllers, the registration or submission of a notification of personal data processing is their first contact with Act No. 101/2000 Coll. and its contents. It is increasingly common that, as a consequence of the submitted notification of personal data processing and particularly the subsequent communication between the Office and the notifier, the notifier reduces the originally anticipated scope of personal data processing to minimum. A number of notifiers are not originally aware of the potential risks of misuse of the processed personal data, particularly sensitive data. Consultations with the Office prior to commencement of personal data processing often lead to a conclusion that a substantially narrower scope of personal data suffices for the declared purpose of processing and, simultaneously, the procedures for personal data processing are further specified during the process.

The number of requests for transfer of personal data to other countries was lower in 2003 compared to the previous year. This fact was undoubtedly caused by application of Convention No. 108, which limits, in Article 12, the duty of data controller to request authorization of the Office pursuant to Article 27 (4) of the Personal Data Protection Act in cases of automated processing of personal data transferred between the parties to the Convention. On the other hand, the Registration Department encountered more generic cases of transfer of personal data, which required thorough investigation, both in administrative proceedings and in the area of transfer of personal data of employees to other countries.

Control Activities of the Office

In 2003, the control activities of the Office were performed according to the control plan and on the basis of incentives and complaints. Inspections were directed and performed by individual inspectors. Certain inspections also involved other employees of the Office.

29 inspections were commenced on the basis of the control plan for 2003 and three inspections on the basis of the control plan for 2003. A total of 26 inspections were completed, of which 3 inspections were commenced during the previous year. One of these inspections was not concluded with legal force, as the controlled entity lodged an appeal against the decision on objections against the inspection protocol. Four inspections commenced in 2002 are being further pursued. Inspections commenced pursuant to the control plan of the Office are usually comprehensive inspections covering all duties relevant for the controlled personal data processing and for activities of the controlled controller and processors. Inspections implemented on the basis of written incentives and findings of the media and other sources were concerned with the duties that are directly connected with an incentive or complaint; in two cases, these inspections were comprehensive. Inspectors of the Office initiated 37 and completed 34 such inspections. One inspection commenced in 2002 was further pursued.

The topics covered by control activities of the inspectors in 2003 included both areas and subjects that attract permanent attention of the general public – individuals and the media – and activities of institutions involving processing of personal data of a high number of data subjects. Inspections were aimed at banks; other financial institutions and insurance companies; city and municipal authorities; publishers; media; businesspersons – including Internet and mail-order businesses; personnel and marriage bureaus; police; advertising agencies and direct marketing companies; administrators of distribution networks and providers of services connected with housing; schools – including universities; telecommunication operators; central state administrative bodies; social-care and health-care facilities; and also one carrier and one operator of postal services. Inspections were concerned with processing of personal data on customers and clients; obliged persons and applicants, employees and family members; and pupils and students; and also of personal data on special-interest persons. Processing of data on special-interest persons was subject to control exclusively with respect to performance of the duties imposed on the controlled entities by law.

Inspections usually revealed breach of several duties imposed on the controllers and processors by the Personal Data Protection Act. Breach of a single duty was ascertained in two cases. No violations of the Personal Data Protection Act were ascertained at twenty controlled entities; shortcomings that did not constitute breach of the duties imposed on the controlled entities by law were ascertained in several cases. Processing subject to the Personal Data Protection Act could not be established during one inspection and personal data processing corresponding to the relevant incentive could not be ascertained in one case.

In the framework of the completed inspections, measures for a remedy were imposed on thirty five controlled entities, of which liquidation of personal data was imposed in eight cases. No measures for a remedy were imposed in relation to nineteen controlled entities; this approach was also taken by the inspectors of the Office in cases where the controlled entities remedied the ascertained shortcomings in the performance of duties in personal data processing during the inspection. The inspectors also verified and controlled performance of the imposed measures for a remedy.

Social security and state social assistance in designated municipal authorities

A comprehensive inspection of the designated authorities was also aimed at the areas of social security and state social assistance in 2003. Employees in the area of social security and state social assistance collect and process personal data of the applicants

for benefits and social-care services on the basis of special laws on social security and related regulations on administrative proceedings.

On the basis of the performed inspections, it can be stated that, although the relevant personal data in the area of social security are managed by employees of various authorities, their deviations are more or less the same.

The following deviations were ascertained in the sense of the Personal Data Protection Act in processing of personal data of the applicants for benefits in social care and state social assistance:

Breach of Article 5 (1) (d) of the Personal Data Protection Act by making copies of documents that are basic documents for administrative proceedings in cases of provision of benefits or services in the area of social care and state social assistance, given the fact that not all data contained in the copied documents are required for assessment and subsequent provision of the benefit within social care or benefit of state social assistance, and thus making copies of these documents including the redundant data could constitute breach of the duty pursuant to Article 5 (1) (d) of the Personal Data Protection Act.

When lodging an application for a benefit of social care and benefit of state social assistance, the contact and identification data of the applicant are verified according to the submitted documents (in particular the personal identity card). It was ascertained during the inspections that the above-mentioned personal data of applicants are also verified in the records of citizens; nevertheless, copies of personal identity cards are made in a number of cases.

Furthermore, unjustified copying of entire statements of bank accounts, which were part of certain files of applicants for a social-care benefit, was ascertained during the inspections.

While, in accordance with the special regulations on social security, when assessing the decisive conditions (in particular, the income; overall social situation and assets of the applicant; other conditions that follow from the special laws for the provision of social-care benefit within administrative proceedings), employees of the social departments of the designated authorities are obliged to verify, document and obtain evidence (in particular, pursuant to Articles 34 and 37 et seq. of Act No. 71/1967 Coll., on administrative proceedings, as amended), pursuant to the Personal Data Protection Act they are obliged to collect only personal data corresponding to the set purpose and within the scope required for attaining the set purpose.

Making copies of some other documents (in particular, the certificate of marriage, birth certificate of a child, court decision on alimony, lease contracts) as documentary evidence, on the basis of which decisive data on the provision of a social-care benefit can be documented, can also be at variance with the Personal Data Protection Act pursuant to Article 5 (1) (d) if a copy of the given document contains also data that are not taken into account in assessing the given benefit and are thus not required, with respect to their scope, for attaining the set purpose.

Furthermore, it was ascertained during the performed inspections that, in cases where the health condition of the applicant is also decisive for granting a social-care benefit pursuant to the special regulations on social security, social workers of certain designated authorities collect data on the health condition to an extent that is not in accord with the special regulations and their processing is at variance with Article 5 (1) (d) of the Personal Data Protection Act.

The health condition of an applicant is decisive for the provision of certain social-care benefits pursuant to the special law. Pursuant to Decree No. 182/1991 Coll., implementing the social security act and the Czech National Council Act on the competence of the bodies of the Czech Republic in social security, as amended, under Articles 1 and 2, assessment of the health condition falls within the competence of the relevant doctor and a doctor of the district (Prague) social security administration.

Thus, according to the special law, workers of social departments of the designated authorities are not competent to assess the health condition of the applicant on the basis of detailed medical reports that formed part of certain controlled files. A decision on granting a benefit pursuant to the special regulation on social security is made by the competent department of the social security body on the basis of assessment and evaluation of the health condition by the relevant doctors pursuant to Decree No. 182/1991 Coll., on proceedings on a social-care benefit or service, and their standpoint.

Inspections also revealed unauthorized collection (processing) of data on the health condition of applicants that were not required for assessing the social-care benefit and were part of the applicant's file. Thus, breach of the duty following from Article 5 (1) (f) of the Personal Data Protection Act had to be noted.

Health Care

Inspections of health-care facilities were commenced in 2003. Attention was concentrated particularly on hospitals that could be characterized as "district" hospitals. Certain investigations were also performed in these facilities outside the framework of state control. Given the scope of these investigations, their results can also be used to supplement and generalize the control findings.

In principle, two groups of ascertained issues should be described.

The first issue is related to protection of personal data in the sense of their organizational and technical securing, particular in connection with the existence of the relevant internal regulations and their quality, compliance with certain security standards, safe operation of information systems in hospitals, and, in general, legal awareness, practical potential and willingness of health-care workers to protect personal data in general.

It can be stated that, in small hospitals, personal data protection is ensured rather intuitively. Data protection is usually perceived from the viewpoint of the confidentiality duty of health-care workers (Article 55 of Act No. 20/1966 Coll., on care for the health of population, as amended) and labor regulations; however, there are no relevant comprehensive measures providing particularly for protection of personal data of patients against access by unauthorized persons. No misuse of personal data, e.g. by means of their systematic theft, unauthorized access to the information system of hospitals, etc., was ascertained. Misuse occurs particularly on the basis of personal deviations of individuals, e.g. unauthorized disclosure of data on newly-born infants from the birth departments to insurance agents, telephonic provision of information to unauthorized persons (e.g. by porters), etc. However, there are also other deviations, such as placement of the results of examinations of patients in an open filing cabinet in the corridor of a hospital, where they were easily accessible by all persons passing by.

The securing of electronic information systems in hospitals probably depends particularly on the financial capacity of health-care facilities. Top priority is given to operation of the system for the needs of the hospital from the viewpoint of the treatment process, while security from the viewpoint of potential misuse is secondary (although not neglected).

Further shortcomings follow from lack of systematic data protection. This can be illustrated by a case where unique data of patients stored in the information system of a hospital are also stored on back-up CDs; however, these CDs are kept in the same building as the relevant servers (thus, in case of a fire, there is a danger of an absolute loss of data). It is a common feature that e.g. access by health-care workers to the information system is conditional upon authentication and authorization (access name and password); however, the passwords usually remain unchanged and their changes are not required. While a situation, where a doctor leaves to attend a patient and full access to the information system of the hospital remains displayed on the monitor, may be generally and professionally understandable from the viewpoint of the doctor, it is unjustifiable in a wider context.

The above-mentioned examples document a very specific aspect of health-care facilities and their employees, particularly doctors, from the standpoint of their approach to personal data protection. The doctors pay attention primarily to medical care for a patient, which is absolutely comprehensible, while other activities are only of marginal interest. This approach should be gradually modified, undoubtedly while retaining the priority of health care.

The second issue, whose importance became fundamental during 2003, is implementation of national health-care registers. These registers are part of the National Health-Care Information System and are regulated in Part Five of the Act on Care for the Health of Population.

It was ascertained that health-care facilities (probably all, without any exceptions) submit personal data to the national health-care registers at variance with the valid legislation. This fact is a fundamental systemic failure of the health-care sector as a whole and could lead to very significant administrative and criminal consequences. Pursuant to Section 67c (1) of the Act on Care for the Health of Population, NHCIS is a single national information system intended:

a) to collect and process information on the health condition of the population and on health-care facilities, their activities and economic management, for the purpose of directing the provision of health care, laying down the concept of the state health-care policy, utilization of information in the framework of health-care research, management of health care and the state statistics;

b) to maintain national health-care registers. Pursuant to Article 67c (2) of the same Act, health-care facilities shall provide information pursuant to paragraph 1 (a) within the scope and in the manner stipulated in a Decree of the Ministry of Health.

Thus, the Act on Care for the Health of Population does not determine the scope and manner of collecting personal data in national health-care registers and also does not authorize the Ministry of Health to stipulate the scope and manner thereof in a Decree (the authorization is concerned explicitly with Article 67c (1) (a), rather than with Article 67 (1) (b)). Furthermore, it is explicitly stipulated in Article 67d (3) of the above-cited Act that access to data in registers, their maintenance, collecting data and management thereof is governed by the Personal Data Protection Act.

It follows from the above that the valid legislation does not regulate the subject of personal data of patients in national health-care registers, their specific scope and manners of processing and also lacks any authorization in this relation.

Nevertheless, on May 29, 2002, the Ministry of Health issued Measure No. 18/2002, stipulating the scope of national health-care registers and imposing on health-care facilities the obligation to provide personal data of patients to these registers, both on the basis of incorrect application of the authorization included in Article 67c (2) of the Act on Care for the Health of Population. The above-cited Measure has no basis in law and, above all, it is not a legal regulation in the sense of Act No. 309/1999 Coll., on the Collection of Laws and on the Collection of International Treaties.

This Measure expired as of December 31, 2003 by operation of law (Section 14 of Act No. 309/1999 Coll).

As a consequence of the above-described state of affairs, during the entire year 2003, health-care facilities provided personal data of patients to national health-care registers unlawfully. Thus, health-care facilities could be subjected to administrative sanctions pursuant to the Personal Data Protection Act and the relevant competent employees of the health-care facilities could also face criminal prosecution for the offense of unauthorized management of personal data pursuant to Article 178 of the Criminal Code.

Furthermore, on December 15, 2003, the Ministry of Health issued Decree No. 470/2003 Coll., stipulating the scope of national health-care registers and imposing on health-care facilities the obligation to provide personal data of patients to these registers, again on the basis of incorrect application of the authorization included in

Article 67c (2) of the Act on Care for the Health of Population. This Decree is a legal regulation, which is a part of the valid legal order. However, if it is complied with and implemented by the health-care facilities, this will again be illegal and at variance with the Personal Data Protection Act.

Further processing of personal data in records of inhabitants

In relation to the findings of the Office for Personal Data Protection of 2002 and in response to the incentives delivered to the Office in 2003, personal data processing within the records of inhabitants kept pursuant to Act No. 133/2000 Coll., on records of inhabitants and birth certificate numbers and amending some laws (the Act on Records of Inhabitants), as amended (hereinafter the "Act on Records of Inhabitants"), was controlled in the framework of three separate inspections. The inspections were aimed at or included control of further processing of personal data within the records of inhabitants by governmental agencies. Violation of the Personal Data Protection Act by five entities, of which three were central governmental agencies, was ascertained during these inspections.

Further processing of personal data obtained from the records of inhabitants is carried out by bodies authorized thereto by law. These bodies become controllers of personal data upon obtaining the data from the records of inhabitants. In processing the personal data obtained from the records of inhabitants, several controlled entities breached the duties pursuant to Article 5 (1) (d) and (f) and Article 13 of the Personal Data Protection Act. One controller also breached the duty pursuant to Article 5 (1) (e) and Article 10.

Controllers P. and L. collected personal data from the records of inhabitants within certain areas of performance of government to examine indemonstrable enquiries pursuant to audit records and controller P. also collected these data to establish ownership titles to properties. The scope of collection must be considered to include collection of data on individual data subjects. The scope that is absolutely essential for the fulfillment of the set objective is determined by the scope of persons, on whom data are to be collected. In the present case, these persons are defined by a certain substantively applicable law; other persons may be involved only in individual justified cases. Collection of personal data on persons who have never been applicants or jointly assessed persons, or obliged persons in the given case, is not collection of personal data corresponding to the set purpose.

This is also valid for S.; however, in this case, collection of personal data from other sources included both their obtaining on the basis of an enquiry through a dialogue within distant access to the information system for records of inhabitants, i.e. through assumption pursuant to the provisions of a special law, and automated generating of transaction data on the assumed data. As an entity obtaining personal data from an information system pursuant to a special regulation, S. is not authorized to collect, transfer and use these data outside the competence stipulated in the given regulation. However, S. collected data from the records of inhabitants also on persons who have never been an applicant or a jointly assessed person.

S. breached the duty of the controller to maintain personal data only for a period that is required for the purpose of their processing by keeping the information system of S. in a manner not permitting liquidation of the individual personal data. The system includes operations concerned with invalidation and filing of data. Consequently, personal data are processed on a permanent basis, i.e. also after expiry of the objective lapse period of three years pursuant to Article 63 of the Code of Administrative Procedure, calculated pursuant to Article 27 of the Code of Administrative Procedure, and after expiry of the deadlines for destruction of documents.

Partial accord of the declared and actually implemented purpose of processing was ascertained on the premises of the controlled entity and at the workplaces of the information system of S. The operability of applications for automated processing is

wider than corresponding to the above-specified purpose. The assumed personal data are processed in the information system of S. also for purposes other than specified (i.e. declared by S. himself): for the purposes of assigning and use of electronic signature, both pursuant to the special law, i.e. in the interest of enabling petitions pursuant to a special law and for the purposes of other personal data controllers and for the purposes of internal administration of the information system of S.

Controllers P. and. L. processed personal data from the records of inhabitants in individual cases even if such processing did not comply with the condition stipulated in Article 5 of the Act on Records of Inhabitants.

The manner of processing of personal data obtained from the records of inhabitants, as proposed and performed by S., results in breach of the duty of S. to ensure prevention of harm to the rights of the data subject and ensure protection against unauthorized infringement of the private and personal life of data subjects. This manner of processing infringes on the right of the data subjects to be informed of processing pursuant to the Personal Data Protection Act, i.e. as stipulated generally in Article 5 (2) and (5), Article 9 and Article 11. This right of the data subject is infringed upon in cases where S. processes personal data by making an enquiry within a dialogue with the information system of the records of inhabitants for the purposes of performing an activity that is not imposed thereon by law. A data subject who fulfills the criteria for the object of search in the records of inhabitants is not and cannot be informed of the fact that his personal data are processed in the information system of S. This information does not follow from any law, is not part of advice pursuant to any legal regulation and is also not disclosed to the affected persons prior to commencement of processing or after commencement of processing.

Findings obtained at control of commercial companies providing credit and loans

One incidental inspection of a commercial company engaged, amongst other things, in the provision of credit and loans from internal resources was carried out in 2003. A complaint submitted by an employee of the company was concerned with negligent management of personal data and collecting sensitive data without registration. These facts were allegedly evidenced by the attached documents containing personal data of the clients of the company.

The company collects basic information on its clients at individual branches and thus the inspection was carried out at three branches of the company. It was revealed that the company has strict rules for management of personal data, keeping records thereof in computers and their potential destruction.

The work assignment of certain employees includes access to personal data of clients whose loans they keep. The present case involved employees who failed to comply with the rules of the company and kept documents at a time when they no longer needed them; one employee even disclosed these documents without authorization. Therefore, a proposal for sanction proceedings for a misdemeanor pursuant to Article 44 of the Personal Data Protection Act was lodged against this employee.

Pursuant to Article 13 of the Personal Data Protection Act, the controller is obliged to adopt measures preventing unauthorized or accidental access to personal data. Thus, within inspection, it must be ascertained what measures the controller has taken to ensure personal data protection. In cases where the work assignment of several employees includes contact with personal data of data subjects (e.g. clients of the company), it must be particularly ascertained whether rules have been adopted for management of personal data and whether the employees have been acquainted with these rules. Thus, if an employee knowingly breaches the internal rules and thus also the confidentiality obligations with an intent to harm the company, blame must be cast on the employee, rather than on the company.

The allegation that the controlled commercial company processed sensitive personal data without the required registration was also not confirmed.

Summary of the results of a set of inspections aimed at processing personal data of customers, users and employees of distribution companies

In accordance with the results of the control activities of the Office for Personal Data Protection in 2002 and in response to incentives delivered to the Office in 2003, processing of personal data of the customers, users (natural persons) (hereinafter the "clients") and employees by various companies that own or manage extensive distribution networks, including networks supplying energy (heat and hot water, electricity or gas), networks distributing drinking water and ensuring the discharge of wastewater into sewerage systems, or networks ensuring transmission of radio and television programs by cable, were controlled in the framework of four separate inspections. The more extensive is the operated distribution system, the more clients the distribution system can have. The numbers of clients of distribution companies can equal tens or hundreds of thousand.

The following findings were obtained through evaluation of the results of these four controls aimed at fulfillment of the duties of controllers in processing personal data of clients of distribution companies and in processing personal data of their employees pursuant to the Personal Data Protection Act:

- Several controlled entities breached the duty to collect only personal data corresponding to the set purpose and within the scope required for attaining the set purpose of processing pursuant to Article 5 (1) (d).
- A single controlled entity violated the obligation to lay down the means and manner of personal data processing pursuant to Article 5 (1) (b). A single controlled entity failed to comply with the obligation to maintain personal data only for the period required for the purpose of their processing pursuant to Article 5 (1) (e). A single controlled entity failed to fulfill the duty to conclude a proper contract with the processor pursuant to Article 6.
- Breach of the duty to process personal data only with the consent of the data subject pursuant to Article 5 (2) and, furthermore, to obtain the consent of the data subject pursuant to Article 9 (a) was frequent, i.e. committed by several entities. Further, several controlled entities failed to fulfill the duty to duly notify the data subjects pursuant to Article 11.
- In a single case it was found that the employees of the controller failed to process personal data only under the conditions and within the scope laid down by the controller, by which the controller violated the provision of Article 14 of the Personal Data Protection Act. Furthermore, violation of Article 15 (1) was ascertained in one case.
- Two controlled entities failed to fulfill the notification duty pursuant to Article 16.
- Lack of legal awareness from the viewpoint of personal data protection was ascertained in relation to several controlled entities.

During the inspections, it was ascertained that Article 13 of the Personal Data Protection Act creates a desirable pressure on distribution companies (controllers) to adopt measures preventing unauthorized or accidental access to personal data.

Processing of personal data by designated municipal authorities

Inspection was performed in three cities with extended competence and a designated municipal authority in 2003. These comprehensive controls were aimed particularly at ascertaining the scope and manner of personal data processing by these entities. Inspection was formally commenced at one of these entities in 2002; however, due to transferring the agenda of the dissolved district authorities, this inspection was immediately suspended and carried out entirely during 2003.

The duty to process personal data is explicitly imposed on municipalities by several dozens of laws. Municipalities are required to process a lot of data in order to be able to

fulfill the duties stipulated by special laws. Municipalities are also employers, the owners of real estate and have to deal with other private relations; they keep approximately 100 separate records containing personal data. The above-mentioned extensive inspections were divided to the following nine relatively separate areas.

1. Records of employees of the municipal authority kept on the basis of special laws.
2. Records of inhabitants and register of births and marriages.
3. Personal data processing in the area of social security.
4. Other personal data processing within independent and delegated competence.
5. Personal data processing imposed on the municipal authority by self-governing bodies.
6. Records kept by the Municipal Police.
7. Publishing of personal data.
8. Compliance with the principles of security of processing.
9. Compliance with the procedures in filing and destroying documents.

It was revealed during the inspections that employees of municipal authorities usually believe that personal data include only identifiers. However, personal data means data that are concerned with a specific and identifiable data subject (i.e. a natural person to whom the data are related). However, the specificity is based rather on subjective aspects; e.g. in a small municipality, a person can be identified on the basis of his name, surname and address; this is, however, impossible in a larger city, where more information is required. The specificity and identifiability is also related to the appropriateness of time, effort and material means required to identify a person (e.g. surname and data on occupation in a large city).

A fundamental issue connected with personal data processing is apparently related to Article 5 (1) (h) of the Personal Data Protection Act which imposes of the controllers the duty "to ensure that personal data that were obtained for various purposes are not combined, unless a special Act stipulates otherwise". Records of inhabitants enable to use the register of inhabitants to perform agendas both within delegated and within independent competence. However, modern information technology that is increasingly used by municipalities also covers all other agendas and allows for their concurrent processing.

The bodies active in criminal proceedings often request that the bodies of municipalities and cities provide them with "reputation reports", within which they require information on the manner of life, behavior, etc., i.e. information that municipalities cannot (and may not) process. Instead of this report, the controlled cities provide information whether the conduct or behavior of the relevant citizen has been discussed by their misdemeanor committee.

Keeping records of discussed misdemeanors or records of persons who have committed misdemeanors is not regulated by law; however, there are some basic provisions in other regulations that require information from an imaginary register. However, these provisions are not concerned universally with all persons who have committed a misdemeanor.

Transparency of public administration is bound on compliance with other laws that undoubtedly include the Personal Data Protection Act. Where a law unambiguously delimits a scope of persons who are entitled to become acquainted with the relevant documents, compliance with this scope cannot be guaranteed when the documents are published on the Internet. In that case, amongst other laws, the Act on Municipalities is undoubtedly violated. The Office for Personal Data Protection is interested in such deviation only if the relevant document contains personal data. In that case, the Personal Data Protection Act unambiguously requires the consent of the affected persons – data subjects. Where the personal data controller – municipality has not obtained such consent, it faces not only a potential sanction imposed by the Office, but also criminal prosecution of the person liable for violation of Article 178 of the Criminal Code

(unauthorized management of personal data). However, it is clear that the current expansion of new technology creates an incentive for making accessible as much information as possible. Municipalities must carefully consider the scope of published data and maintain the required appropriateness, which does not make the relevant information redundant, and thus infringe upon privacy of persons only in justified cases.

The inspections proved an effort to provide a lot of data and services through the Internet. However, a majority of controlled entities fail to implement security measures that would adequately guarantee security of the processed personal data.

Personal data on the Internet

A vast volume of personal data are available on the Internet. These data are publicly accessible at websites, and are also contained in electronic mail and on servers accessible from the Internet. The general public can access personal data of entrepreneurs (the Commercial and Trade Registers), owners of real estate (the Land Register), members of boards of directors and supervisory boards of non-profit organizations, representatives of self-governing bodies, i.e. members of municipal councils of cities and municipalities, often also employees of municipal authorities, and through minutes of meetings of municipal councils, also personal data of persons discussed at these meetings. The thus published data are often used for purposes other than the purpose, for which they were collected and published.

Control was aimed both at publishing of personal data on the Internet by self-governing bodies and the operators of Internet stores. Publishing of personal data obtained from an inadequately secured server was dealt with in one case. Inspections revealed that a majority of controlled entities fail to implement adequate security measures that would guarantee security of the processed personal data. Governmental bodies connect their networks, which also contain very sensitive personal data, to the Internet in a manner that would hardly withstand a qualified attack from outside. However, it is difficult to prove any such attack.

In case of electronic stores, specialized companies that lease the capacity of their transmission lines, servers and application software to other providers of commercial services are usually careful when concluding the relevant contracts. These companies do not consider themselves processors in the sense of Article 4 of the Personal Data Protection Act, although they can access these data, e.g. as administrators. The contracts do not contain adequate security guarantees and, in some cases, the contracts are even conceived so that the companies are not liable even for a potential attack on servers and subsequent destruction or theft of data connected with operation of Internet commerce.

Personal data processing in the banking sector

The banking sector underwent relatively considerable changes in the area of personal data in 2003. As the commercial strategy of banks concentrated more on minor clients, particularly in the area of consumer loans, the banks turned their attention to collection or personal data of their clients and particularly obtaining information on the clients from other sources; they strived to ensure reciprocal provision of personal data of the clients to other, even non-bank entities. This leads to potential violation of the Personal Data Protection Act. On the basis of the Act on Banks (No. 21/1992 Coll.), banks have a number of strong instruments to secure recovery of loans and to ascertain the solvency of applicants for a service they offer. They are e.g. also entitled to publish information on debtors. In relation to securing bank interests, contractual documents are very well prepared; however, these contracts have considerable shortcomings with respect to protection of the rights of the clients – in particular, with respect to the Personal Data Protection Act. This is also reflected in the varying quality of documents submitted for execution to the clients in provision of services in the framework of business activities of certain banks.

The Personal Data Protection Act is most frequently violated by some banks that require the "consent" to activities that are not subject to the Act on Banks and are also outside the framework of the subject of the license issued by the Czech National Bank.

In particular, it is not respected that the consent can be generally granted only on the basis of a civil or other contract (unless the Personal Data Protection Act or other laws lay down otherwise) and, therefore, it is not admissible to order the citizen to agree with all requests of the bank or make the provision of a banking service conditional upon granting such consent. The most frequent deviations connected with requiring the consent in banking sector that have been revealed to date are as follows:

- Inclusion of the consent in the General Terms and Conditions of the bank, which could be at variance with Article 5 (1) (g) of the Personal Data Protection Act.
- Violation of Article 11 of the above-cited Act – i.e. the notification duty, particularly in relation to the voluntary provision of consent, possibility of agreement on other conditions, etc.
- Inclusion of purposes of processing in the consent, for which the bank does not require consent as they directly follow from the Act on Banks or other laws.
- Non-compliance with the particulars of the consent pursuant to Article 5 (5) of the Personal Data Protection Act, particularly in provision of personal data that are subject to bank secrecy to third persons in that the entities, to whom such data are to be provided, are vaguely specified (e.g. by incomplete name), and the purpose and object of their business is not clearly specified; thus, the relevant person is practically not aware to whom his personal data will be provided.
- Inappropriately long periods of time that the banks require within the consent for certain instances of processing even after termination of any legal relationship with the client; unless, the period of time follows from a special law, the banks could be at variance with Article 5 (1) (c) and (e) of the Act, as the data are not updated in these cases.

The banks request the above-mentioned consents for the transfer of data that are subject to bank secrecy, particularly to their subsidiaries, which are then able to address a group of potential clients of the bank in a more sophisticated manner and thus substantially reduce their costs.

Non-banking entities understandably show great interest in data of the clients of banks, as these data allow them to target offers of their products more precisely and thus minimize their costs. However, in this relation, there is a considerable risk of potential misuse of personal data and infringement of privacy both by companies and by individuals who obtain these data without control. Personal data are substantially less secured outside the banking sector – in contrast with the banks, other sectors expend less money to protect their data.

However, it should be noted in this respect that the current legislation does not permit establishment of a register of actual debtors and non-payers (i.e. persons who break contracts) that would be regulated by transparent rules laid down by law and its availability controlled (e.g. by the Commercial Code). The legislators could find inspiration e.g. in SCHUFFA operated in Germany or the Credit Report used in the U.S.A.

Making copies of documents, which is required by banks in concluding contracts on certain provided services, is also problematic. While banks must proceed pursuant to Act No. 61/1996 Coll., on certain measures against legalization of proceeds from crime, which imposes on specified persons the duty to identify and report suspicious transactions, as also required by Directive 2001/97/EC, the valid law does not permit making copies of documents; thus, the copying of personal identity cards, birth certificates, passports and other documents could be qualified as violation of Article 5 (1) (d) of the Personal Data Protection Act. The above-mentioned documents also contain personal data (on the spouse, children, parents, grandparents, vaccination, religion, etc.)

that have no relation to the provided service; these data are thus also copied. As the amendment to Act No. 61/1996 Coll. is currently subject to the second reading in the Parliament of the Czech Republic, inspections, during which copying of documents was established, were suspended in order to avoid any harm to the rights of the controlled banks.

Activities of the Control Department

The main task of the Control Department is to accept complaints and petitions concerning personal data processing and then address these complaints and petitions. Addressing complaints and petitions can include:

- Evaluation of legitimacy of complaints.
- Obtaining available evidence.
- Communication with the complainant and also with the challenged entity, if appropriate.
- Initiation of inspection by an inspector of the Office or commencement of sanction proceedings pursuant to Chapter VII of the Personal Data Protection Act.
- Referring the matter to the bodies active in criminal proceedings.

In 2003, the Control Department dealt with 264 petitions of the above nature.
Of which:
149 cases were closed
34 cases were referred to inspectors
21 cases were referred to the Administrative Decision-Making Department
2 cases were referred to the Police of CR
2 cases were referred to the District State Attorney's Offices
3 cases were dealt with as misdemeanors
53 cases are under investigation

The relevant petitions are assessed very informally in accord with the sense of the Personal Data Protection Act. The complainant need not demonstrate legal interest in the given matter and does not have to comply with any explicit formal particulars.

However, a requirement can be derived from the viewpoint of the purpose of the petition for unambiguous specification of the entity against whom it is aimed and for description of the alleged violation of the Act, as well as for provision of available evidence. On the other hand, a complaint may in no case be confused with a proposal for commencement of administrative or civil court proceedings. Thus, the Office is never bound by the relevant petition and the complainant does not have the position of a party to the proceedings. However, the Office notifies the relevant complainant of the manner of dealing with his complaint and explains to him why his petition cannot be considered legitimate, if appropriate.

In principle, the Office does not reject any anonymous petitions, whose number somewhat increased in 2003. Very frequently the complaints are illegitimate for the reasons of substantive shortcomings or incorrect comprehension of the legal regulation.

A number of complaints have clearly been submitted due to the fact that a certain entity failed to satisfy a certain request of the complainant. Thus, in their nature, many petitions are not primarily related to personal data protection, but were rather modified as such when the complainant was not satisfied in proceedings pursuant to some other regulations or when he came to the conclusion that this process (e.g. court action) would lead to excessive burdens for him. It is symptomatic in this relation that the complainant usually requests immediate commencement of sanction proceedings pursuant to Chapter VII of the Personal Data Protection Act and disagrees with any measures taken by the

Office to remedy the non-compliant state of affairs as obsolete. The Office also often receives a petition with a considerable delay (sometimes even several years). The complaints are frequently formulated very briefly and are based on unilateral and subjective allegations. Therefore, further investigations are required to objectively ascertain the described state of affairs; however, effective control or other proceedings cannot be commenced.

A number of complaints are also lodged without the submitting person first exercising his rights, as required by the Personal Data Protection Act, with an aim to prevent the relevant personal data processing.

In these cases, the Office for Personal Data Protection refers to the need to primarily assert the relevant claims, where any further steps can be taken by the Office only in case of inadequate response of the controller or processor, as appropriate.

The category of complaints that cannot be dealt with by the Office also includes petitions based on the request of the complainant that the Office for Personal Data Protection assess an expert issue falling within the competence of other bodies; by satisfying such request, the Office would exceed its competence. This is typical particularly for cases where assessment of the health condition is requested and where it is claimed that, by alleged non-compliance with the de lege artis procedure, incorrect or redundant personal data have been processed, and also in case where it is claimed that a certain body (e.g. a court) made a certain act at variance with the procedural rules.

However, in these cases, the Office only refers to proceedings according to other regulations provided that it would be legitimate to take further measures only in case of a certain result of these proceedings.

However, there is another important issue. The complaint might not relate at all to the Personal Data Protection Act. It might be legitimate in relation to personal data processing regulated by a law that is a special regulation in relation to the Personal Data Protection Act. While the Personal Data Protection Act imposes tasks on the Office only in relation to the Personal Data Protection Act itself (see Article 2 (2) and Article 29 (1) of the Personal Data Protection Act), this Act also permits that its provisions be modified or specified by special regulations. This is explicitly stated e.g. in Article 5 (1) (f) or (g) of the Personal Data Protection Act and it can also be indirectly derived from other provisions. This is true e.g. for Article 5 (1) (d) of the Personal Data Protection Act, permitting to collect only personal data corresponding to the set purpose, where this purpose (and thus the scope of processed personal data) often follows from special regulations. Consequently, personal data processing that is in accord with special regulations cannot be considered to be a conduct at variance with the Personal Data Protection Act and these complaints are thus often rejected as illegitimate. This also applies to publishing of personal data that is regulated by a special law. In 2003, this could be stated particularly in relation to the following activities:

- Keeping of the Land Registry pursuant to Act No. 344/1992 Coll., on the Land Registry of the Czech Republic (the Cadastral Act), as amended
- Keeping the Commercial Register pursuant to Act No. 513/1991 Coll., the Commercial Code, as amended
- Publishing information on agents of the State Security Force pursuant to Act No. 140/1996 Coll., on disclosure of files established by activities of the former State Security Force, as amended.

A basic problem of many controllers is related to the fundamental lack of conceptual arrangement for personal data processing.

There is still a tendency to collect data without any specific need and without a specifically defined purpose.

The frequently ascertained violation of Article 13 of the Personal Data Protection Act is also caused by the above-described lack of conceptual arrangement. This follows

primarily from unclear formulation of organizational rules for personal data processing. A number of controllers approach the fulfillment of the relevant provision from a purely technical standpoint and provide only for e.g. installation of a certain program equipment or security equipment and absolutely neglect clear stipulation of rules for entering, updating and provision of personal data.

Another related issue consisted in fulfillment of Article 6 of the Personal Data Protection Act in case the controller delegates performance of certain activities in personal data processing to the processor. In these cases, the Office often had to refer to considerable lack of clarity of the terms of the contract between the controller and the processor.

A more general issue is related to the fact that the controllers are sometimes not fully aware of their duty to notify the data subject in accordance with Articles 11 and 12 of the Personal Data Protection Act and do not respond to legitimate requests or respond to them only after intervention by the Office. The Office states that such lack of communication is a frequent reason for submission of complaints to the Office.

An unclear source of data used to address potential clients is a persisting problem in the area of direct marketing. This is probably also caused by the fact that a lot of data were obtained prior to legal force of the Personal Data Protection Act.

Thus, the above problems also document the fact that the opinion according to which personal data are fully at the disposal of by their holder has not yet been fully overcome, while the Personal Data Protection Act is based on the opposite premise according to which it is up to the data subject (subject to exceptions permitted by law) how these data are to be managed.

In this relation, the Office states that the issue of collection, classification and use of e-mail addresses for advertising purposes is a logical result of unregulated and almost uncontrolled development within the Internet.

A relatively new issue is connected with installation of security equipment in dwellings. In order to increase the safety of residents and in the interest of reducing the number of cases of breaking and entering, and of vandalism, the owners and managers of buildings intended for housing often purchase very expensive ready-to-use electronic systems (such as electronic opening of doors using chip cards, monitoring of the premises by a camera, and keepings records of arrivals and departures of the individual residents of the building in a computer program). However, they are not aware that these systems are primarily intended for small and medium enterprises and their purpose is particularly to keep electronic records of attendance of employees, to monitor problematic locations at the workplace, and to file these records for the purposes stipulated by law. However, the relationship between the employer and his employees is based on an entirely different legal provision than the relationship between the manager or owner of a building and the persons residing in the building. While the employer is entitled to monitor compliance with the working hours of employees or their departure from the workplace, the manager of an apartment building has no valid reason to monitor when a tenant or resident of a cooperative apartment arrives at the building or leaves it. It must be a matter of course that the residents of the building are informed of installation of the electronic system. Advanced functions of the system, such as monitoring and keeping records of arrivals and departures with the use of electronic chip cards, can then be used only if the residents of the building provide their consent with particulars required by the Personal Data Protection Act.

The birth certificate number continues to be excessively utilized on the basis of an incorrect opinion that a birth certificate number is an absolute identifier of a natural person and thus a natural supplement to the name and surname. However, the Office for Personal Data Protection bases its considerations on the fact that knowledge of the name, surname, address and the date of birth, as appropriate, fully suffices to identify a natural person. Therefore, processing of the birth certificate number is admissible only where this is laid down by a special law (e.g. for the purposes of social security, etc.).

Otherwise, this is a redundant piece of information processed at variance with the provision of Article 5 (1) (d) of the Personal Data Protection Act. Thus, however, the Office does not preclude introducing a special identifier (e.g. a customer number). It must be noted that knowledge of the birth certificate number can generally be misused for illegal interconnection of individual records leading to unacceptable monitoring of a natural person. However, it should be stated that the excessive use of birth certificate numbers is currently so common that amendment to Act No. 133/2000 Coll., on keeping records of inhabitants and birth certificate numbers, will be clearly required for its elimination, explicitly prohibiting this use and laying down a transitional period to attain a satisfactory state of affairs.

The Office for Personal Data Protection continues to eliminate activities consisting in copying personal documents and subsequent retaining of copies of documents, which is often presented as a precondition for the provision of services. The Office continues to base its activities on the standpoint that personal documents (e.g. the personal identity card) contain substantially more information than required for the conclusion of a contract and thus keeping all information contained in the personal identity card is not admissible. However, in this relation, it must be kept in mind that making copies of personal documents cannot simply be prohibited as processing contra lege, as no clear basis for such a measure has been found in law to date. The recommendation for the data subjects to insist on adequate modification of copies of personal documents, e.g. by blackening, does not indicate unwillingness to impose the required penalties on the controller, but rather that attempts are made to find an acceptable solution for effective protection of the rights of natural persons.

The Office for Personal Data Protection continues to fight against publishing lists of debtors. The Office bases its reasoning on the fact that the relevant procedure is not a legal method of exacting the debt.

A number of controllers continue to attempt to factually evade the provisions of the Personal Data Protection Act through the requirement for the consent of the data subject. Such consent is usually formulated very broadly – in particular, it does not accurately specify, at variance with the provisions of Article 5 (5) and Article 9 (a) of the Personal Data Protection Act, which personal data are to be processed, for what purposes and by which controllers. The period of time, during which personal data will be processed, is frequently not specified or this period of time is inappropriately long. Furthermore, the provision of a certain service is often made conditional upon the consent to processing of personal data for purposes that are not directly related to such service, which is violation of the provision of Article 5 (1) (g) of the Personal Data Protection Act.

A petition was lodged in two cases with the bodies active in criminal proceedings. The Office follows from the fact that it is necessary to prefer an interest in clarifying criminal activities over the proceedings pursuant to the Personal Data Protection Act. However, simultaneously, the bodies active in criminal proceedings were provided with a number of consultations, where the object of their interest consisted in personal data processing.

A number of incentives were also provided by these bodies. These were concerned, in particular, with situations where the case was suspended as the relevant conduct did not have the features of a criminal offense, but where the results of investigation rather indicated that the conduct could point to a systemic defect in personal data processing.

Furthermore, the Control Department fulfilled to a certain degree the tasks of the body competent to discuss sanctions pursuant to Chapter VII of the Personal Data Protection Act. Given the increasing scope of the agenda, the Administrative Decision-Making Department, which was established in 2003, assumed a certain part of supervision over the Personal Data Protection Act within its specialization. The Control Department intensively participated in the preparation of the Office to perform tasks connected with the agendas related to Europol and the Schengen acquis.

Discussion of Misdemeanors and Proceedings on Administrative Torts

The supervisory activities of the Office for Personal Data Protection also include decision-making in relation to liability of the controllers and processors and other individuals for breach of duties stipulated by the Personal Data Protection Act. Since 2003, verification of incentives in the above-mentioned area that are addressed to the Office, as well as of incentives following from its own findings obtained within its control activities, has been entrusted to the newly formed Administrative Decision-Making Department.

Issues that were repeatedly addressed by the Office within investigation of administrative torts included primarily unauthorized publishing or disclosing of personal data. In a number of cases, this tort is aggravated by the fact that the data are published or disclosed by governmental bodies. Activities of these bodies are regulated by law and the scope of their competence cannot be extended, even from the viewpoint of personal data protection, over and above the framework of the regulations that provide for the competence of administrative institutions and that always stipulate, at least in general, the objective and means of management of personal data.

Second frequent violation of the Personal Data Protection Act, which is discussed from the viewpoint of liability for torts, is related to pursuing private activities in the framework of relations that are not regulated in detail by law. A common cause for violation of the Act in this area is the lack of consent required for personal data processing and also inadequate provision of information to the data subject in relation to the manners of management of his personal data.

Statistical results characterizing the activities of the Office in discussing misdemeanors and in holding proceedings on administrative torts in 2003 are given in the following table.

Total number of incentives related to suspected administrative torts	72
of which based on own findings	21
on the basis of referral by the bodies active in criminal proceedings and bodies dealing with misdemeanors	9
on the basis of incentives of natural and legal persons	42
Addressed	
through discontinuation prior to commencement of proceedings	11
through a decision on imposing a fine	17
of which with legal force	9
discontinuation of proceedings	0
referral to some other body	2

Foreign Relations and Participation of the Office in International Cooperation

In the area of foreign relations and international cooperation, the Office continues primarily to provide for fulfillment of requirements following from international treaties binding on the Czech Republic, as stipulated in Article 29 (1) (g) of the Personal Data Protection Act. In connection with performance of the European (Association) Agreement, in the framework of its competence, the Office provides for harmonization of the national legislation and the related practice with the law of the European Union, the acquis communautaire. In a fundamental document of the European Commission, consisting in the last year prior to accession of the Czech Republic to the European

Union in the Comprehensive monitoring report on the state of preparedness for EU membership of the Czech Republic, it is stated in Chapter 3 – Free Movement of Services that: "The Czech Republic has substantially harmonized its legislation in the area of personal data protection and free movement of these data. Nevertheless, certain modifications are required to harmonize the Personal Data Protection Act and the Act on Banks. The Office for Personal Data Protection has demonstrated that it is fully independent and efficient. Further employees will be required to ensure sustainable operation in the long term." In relation to Chapter 24 – Matters of Justice and Interior, there is a more favorable evaluation of the state of harmonization of the legislation; however, the need for increasing the headcount by further recruiting is again mentioned.

In connection with the notes on the need on certain "modifications" of the Personal Data Protection Act, the Office has drawn up a draft amendment to the Act that should ensure final transposition of Directive 95/46/EC and simultaneously eliminate the incompatibility of Act No. 21/1992 Coll., on banks, as amended, from the viewpoint of personal data protection. The draft amendment to the two Acts that was submitted to the Government of the Czech Republic on September 30, 2003 was based particularly on the results of working contacts with the relevant workplace in the framework of DG Internal Market of the European Commission and also on certain results of cooperation with Spanish experts in the framework of the Phare twinning project, which was completed in 2003. The Office cooperated with the Ministry of Informatics of the Czech Republic on transposition of the more recent legal regulation affecting the area of personal data protection - Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. In the framework of the European Union, the Office not only maintains contact and cooperates with the above-mentioned DG Internal Market of the European Commission, but a representative of the Office also participated in four meetings of the Committee pursuant to Art. 31 of Directive 95/46/EC, which is part of the European Commission and in which individual member countries are usually represented by a delegate of the governmental body responsible for implementing the governmental policy in the area of personal data protection. This has not yet been dealt with in the Czech Republic and in a number of other Accession Countries from the viewpoint of competence. The same is valid for cooperation in the framework of COREPER, where the Office "substitutes" for a governmental body, although it has not directly participated in its meetings to date. The Office directly cooperates particularly with the Ministry of Interior of CR and the Ministry of Finance of CR. Cooperation was developed especially with the Ministry of Interior of the Czech Republic in preparation of activities connected with the Schengen Agreement and Europol Agreement. These activities are concerned with future important and difficult agenda that will require specific solutions, both in the framework of domestic control activities and from the viewpoint of international cooperation. In addition, the Office should be represented in the joint supervisory bodies (the Joint Supervisory Body and the Joint Supervisory Authority) in Brussels, which are active in connection both with the two above-mentioned Conventions within the competence of the Ministry of Interior of CR and with the Convention on the Use of Information Technology for Customs Purposes, which falls within the competence of the Ministry of Finance of CR (the General Customs Directorate). Representatives of the Office have already participated as observers in a number of meetings of all three joint supervisory bodies.

The continuing participation of the Office in activities following from the obligations of the Czech Republic as a member state of the Council of Europe and OECD is also related to fulfillment of the requirements of the international agreements. In 2003, the Czech Republic also ratified the Additional Protocol regarding supervisory authorities and transborder data flows related to this Convention and extended the ratification of the original Convention also to non-automated personal data processing. The Additional

Protocol will enter into effect internationally after its ratification by the fifth country; the Czech Republic has been the fourth and the last country to ratify the Protocol to date. The President of the Office represented the Czech Republic in the Council of Europe in the project group on data protection and was also an elected member of the coordination committee. The President participates in the long term in creation of documents of the Council of Europe in this area and has been entrusted with creation of documents on the protection of personal data in the use of chip cards. At the end of 2003, the CJ-PD working groups terminated its activities and its agenda was transferred to the Advisory Committee established pursuant to Convention No. 108 (T-PD), which is the supreme body of the Council of Europe dealing with data protection; at this occasion, the President of the Office, RNDr. Karel Neuwirt, was elected as the senior vice-chairman of T-PD. On request and on the basis of authorization by the Council of Europe, the Office organized a workshop in Prague for employees of the newly established supervisory body for data protection in Bosnia and Herzegovina.

In the framework of OECD, cooperation is also continuing with the Working Party for Information Security and Privacy (WPISP under the ICCP committee). The special importance of the OECD platform and events organized by it lies in the acquisition of valuable information on approaches to data protection outside Europe and on the potential for employing self-regulating instruments in the given area, such as codes of ethics, alternative settlement of disputes, technology supporting privacy, etc. An important contribution of OECD is anticipated in relation to the very sensitive and topical issue of seeking a balanced approach to the legitimate attempts to increase security in relation to the growth of terrorism, on the one hand, and protection of certain democratic values, such as the right to privacy, on the other hand.

During the previous period, the Office fully utilized the extremely important new platform for contact of representatives of independent supervisory bodies at the highest level (usually presidents and/or their deputies) of the EU Member States and the Accession Countries, the Working Party pursuant to Article 29 of Directive 95/46/EC (WP 29).

During the year, representatives of the Office participated in a number of international events, within which they held working meetings with the representatives of partner institutions of the EU Member States and other European and non-European countries. In addition to the above-mentioned meetings of WP29, the most important meetings in this respect included:

- Spring Conference of European Data Protection Commissioners, Sevilla, April 3 – 4, 2003
- 4th Meeting of the Data Protection Commissioners from Eastern and Central Europe, Budapest, April 28 – 29, 2003
- 25th International Conference of Data Protection and Privacy Commissioners, Sydney, September 10 – 12, 2003
- 5th Meeting of the Data Protection Commissioners from Eastern and Central Europe, Berlin, November 6 – 7, 2003

The above-mentioned extensive project of bilateral above-standard cooperation with the Spanish Agency for Protection of Data (APD), which was financed from the National Phare Program, and which was completed in September 2002, was an indirect basis for a new “twinning light” project commenced in 2003, agreed with the same foreign partner and again financed from the Phare funds. This six-month project commenced in September 2003 should provide the Czech Office with experience and knowledge required to fulfill its tasks in the area of electronic communication, the Schengen cooperation, Europol and customs information systems.

In addition to the above-mentioned activities, representatives of the Office participated in over 30 international conferences, workshops and meetings.

The Office, Media and Means of Communication

The frequency of contacts of the Office with the media is described in the attached table. With respect to their quality, it can be stated that a majority of cases where the journalists enquired the Office as to whether a case investigated by them involved violation of the Personal Data Protection Act indeed involved a serious violation of the Act or complex cases that required investigation on site. In several areas – such as health care, electronic communication, monitoring of employees at their workplace, biometry – the media repeatedly showed interest in the issue of personal data protection. It could thus be stated that the media were an important link between the general public and the Office.

The regular quarterly press conferences of the Office not only summarize the work performed by the Office in legislative and legal areas, within control activities, and pursuing international contacts, but usually turn into a more thorough discussion on personal data protection. In addition, they contribute to extending the knowledge of journalists who turn up in relatively high numbers.

Publishing activity and dissemination of new European and global findings in the field of personal data protection

In 2003, the Office published editions 22 – 29 of the Journal, within which it provided a survey of permitted instances of personal data protection and cancelled registrations in accordance with the duty imposed thereon by the Act (Article 35 (2)). As the Office pledged, it also gradually published translations of all important Recommendations of the Council of Europe concerning personal data protection and Directive 2002/58/EC of the European Parliament and of the Council on privacy in electronic communication. Subsequently, it commenced publication of translations of documents issued by the expert group of personal data protectors attached to the European Commission established pursuant to Article 29 of Directive 95/46/EC. In its Journal, the Office also published translations of resolutions adopted at the International Conference of Data Protection and Privacy Commissioners held in September 2003 in Sydney, and provided information on publications with fundamental importance for personal data protection and privacy.

Three new issues of the information bulletin of the Office both provided information to the general public on the quarterly balance of work of the Office and attempted to provide a certain structured picture of personal data protection at the present time (privacy on the Internet, privacy at the workplace, privacy and electronic communication).

However, the most important publishing feat in the area of personal data protection in 2003 was certainly publication of two books written by employees of the Office for Personal Data Protection: The book entitled Personal Data Protection Act – Commentary, written by JUDr. Alena Kučerová, JUDr. Václav Bartík, JUDr. Jaroslav Peca, RNDr. Karel Neuwirt and JUDr. Josef Nejedlý was published by C. H. Beck, and the book entitled Personal Data and Their Protection, written by PhDr. Miroslava Matoušová and Mgr. Ladislav Hejlík was published by ASPI Publishing.

The website of the Office (www.uoou.cz) serves both for the media and for the general public as a reference and basic source of information on the work of the Office, its activities in the Czech Republic and abroad, and on the development in the area of personal data protection in this country and abroad. It contains, amongst other things, a glossary of the President of the Office, where he responds to the current issues in the area of personal data protection dealt with in the media.

Library of the Office

The Office obtained new working premises and thus it was able to establish a specialized sectoral library. The library includes basic literature concerned with personal data protection, as well as the legal aspects of protection of human rights in general, and relevant foreign publications that are undoubtedly unique in a number of cases in the Czech Republic. During the year, the library was extended by 390 documents, of which 220 were purchased; the remaining books were obtained by the Office either as a gift or by exchange. At the present time, the Library has 1020 items of professional sectoral and basic literature (dictionaries, encyclopedia, etc.).

Periodicals offered by the library include the daily press and 30 professional journals.

The library is conceived as an on-site facility and enables primarily the employees of the Office to study the relevant materials. Of course, it also offers its services to external interested professionals. These services have already been used e.g. by law students who sought information and reference for their specialized theses concerning personal data protection. The library, with its modern facilities, is fully prepared for future development.

Creation of a visual style of the Office

During 2003, the Office was gradually provided with materials based on the logotype of the Office that was created during the last year. These materials are prepared on the basis of a special graphic manual for the visual style of the Office for Personal Data Protection. This visual style was created by a student from the graphic design and visual communication atelier of the Academy of Arts, Architecture and Design, the winner of a tender for the logotype of the Office.

The Office uses the above-mentioned design of materials in cases where it does not act within the obligatory legal agenda that is strictly subject to formal particulars. Of course, within performance of its competence, it continues to use state symbols.

Communication of the Office with Media in Figures

Period: January – December 2003

Agency service	16
Total press	102
Of which:	
Daily press	63
Periodicals	39
Television	55
Radio	30
Basic documents for the media	89
Total media	292

Administration of the information system

A number of changes occurred during 2003 from the viewpoint of informatics. The entire area of informatics was reorganized in connection with moving the Office into a new building. The new Informatics Department was created from the former Information System Administration Department. In connection with moving the Office during the month of January, the Informatics Department was presented with the task to move the entire office and computer equipment and to put the information system of the Office into operation as quickly as possible. This was achieved during less than 3 days.

Currently, the employees of the Office can use the information system for a majority of their working tasks. From the viewpoint of program equipment, the system consists both

of an application that supports keeping of the Register of Permitted Instances of Personal Data Processing and of applications supporting the area of salaries and financial management, as well as of auxiliary applications, such as the Journal, Register of Personal Data Controllers on the website of the Office, legal systems, etc. Of course, the principal application is the program equipment intended for keeping the Register of Permitted Instances of Personal Data Processing, which is kept by the Office on the basis of the Personal Data Protection Act. The objective of this application is to support, where practicable, all working tasks connected with registration of "Notifications of Personal Data Processing", including processing of applications for transfer of personal data to other countries, and it is continuously developed on the basis of new requirements.

Another task that was fully accomplished was to maintain an up-to-date and fully operational website of the Office.

During the second half of the year, a survey was carried out, in cooperation with the general contractor for the information system, among selected employees of the Office, concerned with the requirements of the individual departments of the Office on the properties of a product covering the filing service of the Office. Suitable products will be selected on the basis of this survey and a decision will be made on the most appropriate strategy for introducing the selected system.

Organizational measures and a change in contractual relations with the contractors made during the year led to reduction of the costs of data and voice communication services. All requirements of the inspectors and employees of the Control Department for cooperation in control activities of the Office were met.

During the year, employees of the Informatics Department provided for supplementing the required computer and office equipment and provided a sound system for the conference room of the Office.

In addition to participation in a number of professional workshops covering professional issues related to the operation, reliability and security of information systems in institutions, employees of the Informatics Department also participated during the year in several workshops concerning direct protection of personal data.

Personnel of the Office

As of December 31, 2002, the Office for Personal Data Protection had 71 employees. On the basis of Act No. 517/2002 Coll., implementing certain measures in the structure of central state administrative bodies and amending some laws, the agenda and all duties performed by the Electronic Signature Department of the Office for Personal Data Protection were transferred to the newly established Ministry of Informatics, including transfer of rights and obligations following from employment relations of the employees of the Electronic Signature Department.

As of January 1, 2003, the Office for Personal Data Protection had 63 employees. As of March 31, 2003, RNDr. Jiří Souček DrSc. resigned from the office of inspector of the Office in connection with his further activity at the Charles University. Through appointment of Doc. RNDr. Kamila Bendová, CSc. to the office of inspector by the President of the Czech Republic on June 6, 2003, the number of inspectors of the Office was again increased to seven, in accordance with Act No. 101/2000 Coll., on personal data protection.

During the year, new employees were recruited particularly for the newly established Administrative Decision-Making Department and to supplement the personnel of the Legislative and Legal Department according to the set number of employees. As of December 31, 2003 (as of January 1, 2004), the Office for Personal Data Protection had 70 (71) employees.

The Office for Personal Data Protection in Figures – 2003

Lectures, seminars	56
E-mail enquiries	892
Enquiries received by mail – legal persons	510
Enquiries received by mail – natural persons	424
Telephone enquiries	4 044
Total enquiries	**5 870**
Personal consultation – Consultations provided to citizens and institutions	290
Contact with the media – Agency service, press, radio and television	292
Press conferences – Regular press conferences of the Office	4
Materials published:	
Journal of the Office (number of editions)	8
Bulletin of the Office (number of editions)	3
Positions / On practical issues	– / 1
Translations of foreign documents	12
Press releases and communications for the press	10
Additional basic documents for media	89
Total materials published	123
External hits of the website of the Office – daily average	95
Registration – Total number of registrations	3 082
Commented legislative drafts	
Acts	77
Decrees	74
Regulations of the Government	26
Parliament documents	9
Other	41
Total commented legislative drafts	**227**
Institutions on whose materials (not only of legislative nature) comments were provided	
Czech National Bank	5
Czech Mining Authority	1
State Office for Nuclear Safety	1
Czech Geodetic and Cadastral Office	3
Czech Statistics Office	4
National Security Office	4
Industrial Property Office	1
Office for the Protection of Competition	2
Administration of the State Material Reserves	2
Office of the Government	15
Ministry of Informatics	25
Ministry of the Environment	12
Ministry of Labor and Social Affairs	24
Ministry of Transport and Communications	10
Ministry of Interior	31
Ministry of Defense	1

Ministry of Foreign Affairs	24
Ministry of Education	10
Ministry of Justice	22
Ministry of Health	56
Ministry of Finance	21
Ministry for Regional Development	9
Ministry of Culture	2
Ministry of Industry and Trade	2
Ministry of Agriculture	3
Total commented materials / Institutions	**290 / 25**

Transfers of personal data - Number of decisions concerning transfer of personal data to other countries (Article 27 of Act No. 101/2000 Coll.)	89

(The table depicts the state of affairs as of December 31, 2003.)

THE OFFICE FOR PERSONAL DATA PROTECTION
PPLK. SOCHORA 27
170 00 PRAGUE 7
CZECH REPUBLIC
TEL.: + 420 234 665 111
FAX:: + 420 234 665 444
E-MAIL: INFO@UOOU.CZ
WWW.UOOU.CZ