FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions Poland

Zbigniew Hołda
Adam Bodnar
Anna Śledzińska
Piotr Kładoczny
Dominika Bychawska

[Warsaw] [Poland]
February 2009

Contents

Executive summary **3**

Sanctions, Compensation and Legal Consequences **4**

1. Overview **6**
- 1.1. Constitution 6
- 1.2. Law on Protection of Personal Data 7
- 1.3. Compatibility of the Polish Law on Data Protection with the Directive 95/46/EC 11
- 1.4. Data protection in electronic communication 14

2. Data Protection Authority **16**
- 2.1. General Information on the General Inspector for Protection of Personal Data 16
- 2.2. Powers of the General Inspector in the light of the Directive 95/46/EC 20
- 2.3. Remit 24
- 2.4. Allocation of resources vis-a-vis effectiveness of GIODO 24
- 2.5. Guarantees of independence 25
- 2.6. Activity 26
- 2.7. Monitoring 27
- 2.8. Availability of decisions and reporting 27
- 2.9. Working Group Article 29 28
- 2.10. Advisory role 28
- 2.11. Awareness raising role 29

3. Compliance **30**
- 3.1. Administration of information security 34

4. Sanctions, Compensation and Legal Consequences **38**
- 4.1. Protection of personal data in employment relationship 43

5. Rights Awareness **46**

6. Analysis of deficiencies **48**

7. Good practices **51**

8. Miscellaneous **52**

Annexes **53**

Executive summary

Overview

[1]. Personal data is protected in Poland under Article 47 and 51 of the Polish Constitution, the 1997 Law on the Protection of Personal Data, as well as under a number of different special laws regulating some branches of government. The Data Protection Law is modelled on Directive 95/46/EC in terms of adopted definitions and solutions applied.

[2]. The EU law on data protection, including the Directive 95/46/EC is to great extent correctly implemented into Polish law. There are only some small discrepancies between the text of the Directive and Polish provisions.

Data Protection Authority

[3]. Data Protection Authority in Poland is the General Inspector for the Protection of Personal Data (*Generalny Inspektor Danych Osobowych, GIODO*) established under the 1997 Data Protection Law. The General Inspector is not a constitutional organ, and this fact limits its powers and possibilities to have impact on decisions and practices. The General Inspector is appointed by the lower house of the Parliament (*Sejm*) for 4 years term and in this respect it would be difficult to dismiss before the lapse of term.

[4]. The General Inspector is responsible for undertaking different actions concerning data protection, including monitoring of institutions, commenting on laws and giving decisions in individual cases.

[5]. There are ideas to increase the powers of the General Inspector by covering also issues of access to public information and by adding some additional instruments.

Compliance

[6]. The General Inspector has broad powers to make controls and inspections in various public and private entities. It uses this competence quite often and its controls result in different recommendations. It is for this reason that the General Inspector has a positive impact on the protection of personal data by entities being subject of control.

Sanctions, Compensation and Legal Consequences

[7]. The General Inspector has different types of sanctions in order to promote protection of personal data. The most important ones are criminal sanctions. However, in practice they are often ineffective because prosecutors rarely take and litigate cases concerning data protection. Furthermore, the General Inspector does not have a right to enforce its administrative decisions by means of administrative penalties.

[8]. One may expect that in the future the most important sanction against violation of personal data would be through private law instruments and/or– civil law suits.

Rights Awareness

[9]. There are no detailed studies on data protection rights' awareness in Poland. However, the General Inspector undertakes numerous efforts in order to promote the protection of personal data and, thus, to increase public awareness in this field.

Analysis of deficiencies

[10]. The General Inspector has following deficiencies:

- lack of legislative initiative,
- lack of possibility to challenge unconstitutional laws before the Constitutional Court,
- relatively weak position among different governmental bodies and lack of final say on legislation encroaching upon data protection,
- lack of strong enforcement mechanisms of its decisions and orders.

[11]. There is a presidential draft law amending the Data Protection Law which aims towards resolving some of these problems.

Good Practice

[12]. The General Inspector is actively engaged into promotion of data protection and privacy. For this purpose it cooperates with a number of public and private institutions, including universities.

[13]. The General Inspector created a special portal allowing to access and to submit information on data protection through the web.

1. Overview

1.1. Constitution

[14]. Article 51 of the 1997 Constitution of Poland stipulates the right to personal informational autonomy[1]. It specifically provides for the right not to disclose any information concerning one's person unless the obligation to disclose is established in a statute (i.e. act of Parliament); the right to access any official documents and data collections concerning one's person unless an exception is provided in a statute and the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to a statute. These are constitutional norms setting up a general standard of data protection by public authorities[2].

[15]. Other, non-governmental subjects acquiring, collecting or making accessible personal data fall under statutory regulation established in the Law on Protection of Personal Data [*Ustawa o ochronie danych osobowych*, hereinafter referred to as the **"Data Protection Law"**][3]. Interference with the informational autonomy outside the public sphere can however call upon other constitutional rights like the right to privacy guaranteed in Article 47 of the Constitution[4] and to freedom and privacy of communication guaranteed in the Article 49 of the Constitution[5].

[16]. Other constitutional rights – right to information[6] and freedom of economic activity[7] - can be restricted in the process of judicial balancing if they collide

1 Information concerning one's person is considered as personal data. The Constitution is silent about protection of data of other subjects than citizens (individuals).

2 Art. 51 para 2: "Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law".

3 Law of 29 August 1997 on Protection of Personal Data, *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dziennik Ustaw* [Journal of Laws], No. 133, Item 883.

4 Art. 47: "Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life".

5 Art. 49: "The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute".

6 Art. 54 para 1: „The freedom to (...) acquire and disseminate information shall be ensured to everyone"; Art. 61 para 1: "A citizen shall have the right to obtain information on the activities of organs of public authority as well as persons discharging public functions. Such right shall also include receipt of information on the activities of self-governing economic or professional organs and other persons or organizational units relating to the field in which they perform the duties of public authorities and manage communal assets or property of the State Treasury".

with the right to personal informational autonomy. On the one hand, the public right to know (thus, to impart information of public interest, as well as gaining access to public information) can be realized through journalistic activity.

[17]. According to the Press Law[8], it is prohibited to publish information concerning private life of an individual without consent unless it is related to public activity of such person. Privacy of individuals and business secrets restrict right to access public information unless information concerns persons holding public function, related to exercise of this function, or the natural person or the entrepreneur waives its rights. On the other hand, freedom of economic activity implies parallel guaranties of transparency of business operations. Second, rules on consumer's protection entail limited protection of data of business entities.

[18]. In Poland, protection of data of legal persons is covered only by provisions of the Civil Code related to protection of so-called personal rights (*dobra osobiste*). Referring legal persons to a civil suit might be considered as a deficiency (in particular in the light of the Explanatory Memorandum to the OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data) in particular if it concerns illegal processing of such data as trade name, which reveals the first and the last name of the company owner, or the company address being at the same time the owners' address. To make an absolute distinction between protection of natural and legal persons in such cases is neither practical nor rational. Notwithstanding the demand for transparency in business life, the distinction puts an additional burden on legal entities and limits the scope of available remedies.

1.2. Law on Protection of Personal Data

[19]. The Data Protection Law has been adopted in August 1997 and later amended in 2001 and 2004. Protection of personal data prior to the adoption of the Law was not complete in the Polish law and based mainly on protection of personal rights in the Civil Code (Art. 23 and 24), as well as laws on acquiring, collecting and making accessible information in different spheres of life. Such fragmented state of regulation was not compatible with standards of data protection existing in the European Union and Council of Europe.

[20]. The Data Protection Law was modeled on the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on

[7] Art. 22: "Limitations upon the freedom of economic activity may be imposed only by means of statute and only for important public reasons".

[8] Press Law of 26 January 1984, *Ustawa z dnia 26 stycznia 1984 r. – Prawo Prasowe, Dziennik Ustaw* [*Journal of Laws*] No. 5, item 24, as amended.

the free movement of such data[9], as a part of harmonization of Polish law with the law of the European Community in the process of fulfilling requirements under the Association Agreement and preparing for membership to the European Union. Protection of personal data provided under the Directive is more comprehensive than under the Council of Europe Convention No. 108[10]. Because of that, Polish efforts to pass data protection laws were more aimed to harmonize Polish law with EU law than only to ratify the aforementioned Convention.

[21]. The Law entered into force on 30.04.1998. On 23.04.1998, the first Polish General Inspector for Personal Data Protection [hereinafter referred to as the **"General Inspector"**], Mrs Ewa Kulesza, has laid down the oath in the Polish Parliament.

[22]. The activity of the General Inspector has concentrated in the beginning on answering complaints of citizens and issuing administrative decisions concerning breach of provisions on protection of personal data, interpreting the Data Protection Law, as well as issuing opinions on legislative drafts concerning personal data, keeping the register and conducting inspections of data filing systems and providing information on the registered data files. The General Inspector has also played an important role in signaling to administrative bodies laws or practice being incompatible with the Data Protection Law.

[23]. Comprehensive regulation of data protection in one statute (Data Protection Law as *lex generalis* regarding all forms of personal data processing by both public and private subjects) in addition to data protection provisions in different fields of law (several statutes and regulations being *lex specialis* to the Data Protection Law[11]) was regarded as a form of encroachment upon the traditionally deregulated area. This fact is according to some writers the main

[9] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995.

[10] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108. The Convention was ratified by Poland on 24 April 2002.

[11] The specific regulation of data protection concern among others such fields as: civil status acts; population registry, IDs and passports; Polish citizenship; immigration, visa, asylum; education; employment; social insurance, insurance activity, pension funds; social security, health care; accountancy, tax; state control and fiscal audit; money laundering prevention and corruption fight; banking, investment funds; road traffic, drivers' registry, transport; statistics, archives, lustration; telecommunication, electronic services; elections, referenda; public information, press activity; economic activity, business registers; real estate registry; public safety and order; judicial system; army and secret intelligence service, state and official secrets.

problem of present misinterpretation, wrong or lack of implementation of certain data protection rules in Poland[12].

[24]. For the purpose of the Data Protection Law, personal data means

'any information relating to an identified or identifiable natural person'.

[25]. However, in practice doubts arise as to a question what sort of information is actually identifying a person. For example the e-mail address constitutes personal data and falls under protection granted by the Law only when it allows for identification of a person[13]. Thus, posting a private non-identifiable e-mail on the dating Internet portal without the person's consent requires intervention of the public prosecutor. The General Inspector does not have competence to investigate a case unless it concerns "personal data".

[26]. The Data Protection Law establishes that personal data can be processed only in situations and upon conditions foreseen in this legal act. The Data Protection Law rejects the proposal that consent of data subject suffice for lawful collection and use of personal data in specific circumstances and that processing of data is a natural consequence of undertaking economic activity. Importantly, the Data Protection Law does not apply to press/journalistic activity, literary and artistic activity *'unless the freedom of expression and information dissemination considerably violates the rights and freedoms of the data subject'*[14].

[27]. The Data Protection Law stipulates the right of data subject – among others the right to control processing her/his personal data when they are processed within a data filing system. However, the data subject does not have any specified rights when processing of data takes place outside such system.

[28]. The Data Protection Law provides that data processing shall follow principles of:

- lawfulness,
- purposefulness,
- material accuracy,

---

12 See: J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz do ustawy o ochronie danych osobowych*, Lex 2007, p. 119.

13 The example of identifiable e-mail address is John.Smith@coe.int and non-identifiable address, thus formally not a data under the Polish law, is johnys@gmail.com. It would be advisable that also processing of non-identifiable e-mail address equally falls under the scope of investigation powers of the General Inspector.

14 *Cf* Art. 3a para. 2 of the Data Protection Law. Nevertheless, the Law applies to such activity in respect to supervision of the General Inspector and the duty to secure personal data.

- adequacy, and
- time limits.

[29]. The obligations of controllers of personal data include providing information to data subjects, ensuring lawfulness and thoughtfulness of data processing, keeping confidentiality of data and notifying the system to the General Inspector for registration. Furthermore, the controller appoints an administrator of information in charge of compliance with security principles set in the Law or caries out this duty him/herself.

[30]. According to the Data Protection Law, any controller is obliged to notify a data filing system to the General Inspector for registration. However, there are several exceptions from this rule. Importantly, in 2005 there has been an amendment to the Law, stipulating that processing of sensitive data can be commenced only after a data filing system has been duly registered.

[31]. The comprehensive character of the Data Protection Law means that it establishes one standard of protection for all sorts of data irrespectively of the public or private nature of the subject processing the data. Except two categories of data (sensitive[15] and non-sensitive), the Data Protection Law uses a term *'publicly available data'*. Processing of publicly available data is exempted from the registration duty. Such data may also be transferred to a third country notwithstanding the level of data protection ensured therein. Sensitive data can be processed when they are publicly disclosed by a concerned person. Moreover, their processing is allowed for scientific purposes[16].

[32]. According to Article 29 para. 2 of the Data Protection Law:

> 'Personal data, exclusive of data referred to in Article 27 paragraph 1 [*sensitive data*], may also be disclosed, for the purposes other than including into the data filing system, to persons and subjects other than those referred to in paragraph 1 above [*persons or subjects authorised by law*], provided that such persons or subjects present reliably their reasons for being granted the access to the data and that granting such access will not violate the rights and freedoms of the data subjects'.

[15] According to Art. 27 of the Data Protection Law, it is generally prohibited to process sensitive personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings".

[16] The Law provides also for further facilitations for the controllers of data processed for scientific research (Art. 25, 26 para. 3, 32 para. 4). Other facilitations concern processing data necessary for public opinion and for archival purpose.

This provision seems to be too lax since granting access to the data should be permitted only for the purpose of securing public order. Thus, 'presenting reliably the reasons' should not be an independent condition to grant such access.

1.3. Compatibility of the Polish Law on Data Protection with the Directive 95/46/EC[17]

[33]. In principle, the Data Protection Law is compliant with Directive 95/46/EC. However, there are some differences in regulation at the national level of these aspects where Directive 95/46/EC does not leave the margin of appreciation to the states.

[34]. Directive 95/46EC does not apply to situations when data processing concern public security, defence, state security (including the economic well-being of the State when the processing operation relates to state security matters) and the activities of the state in areas of criminal law. The Data Protection Law does not provide for such a general exclusion.

[35]. According to the Data Protection Law, its provisions bind all subjects *'having the seat or residing in the territory of the Republic of Poland or in a third country, if they are involved in the processing of personal data by means of technical devices located in the territory of the Republic of Poland'*. According to the Directive the seat of a subject is established with the reference to a place of *'the effective and real exercise of activity through stable arrangements'*. Thus, the legal status of the subject processing data (whether simply branch or a subsidiary with a legal personality) does not matter.

[36]. Further, there are the following differences with respect to provisions on legitimization of the data processing:

- the Data Protection Law states 'processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision' (Art. 23 para. 1.2), whereas Directive 95/46/EC states that it is necessary for 'compliance with a legal obligation to which the controller is subject' (Art. 7 c);
- the Data Protection Law states that 'processing is necessary for the purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject' (Art. 23 para.1.5), whereas Directive 95/46/EC states 'processing is necessary for the purposes of the legitimate interests pursued

[17] After: J. Barta et al., op. cit., p. 142.

by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection';

- the Data Protection Law seems to exclude a form of consent *per facta concludentia* (Art. 7.5). Also, the Data Protection Law does not mention that information rights of data subject should be accomplished 'without constraint at reasonable intervals and without excessive delay and expense'. The Data Protection Law expands the exemption from the duty to notify the data subject about the processing of her/his data to situations when processing is for didactic and archival purpose (Art. 32 para. 4).

[37]. There is some uncertainty regarding the material scope of the Data Protection Law[18] and the definition of a data filing system that requires registration. According to the Data Protection Law, it is 'any structured set of personal data which are accessible pursuant to specific criteria, whether centralised, decentralised or dispersed on a functional basis" (Art. 7.1). It follows that except subjects expressly exempted by the Law, all public subjects and offices operating any sort of chancellery (electronically or not), including Chancellery of Sejm, Senate, President, the Prime Minister, the Prosecutor's office, courts, etc., fall under the duty to register data processing to the General Inspector. This means that all public subjects in Poland should register their filing systems, which as such have been created to fulfil their statutory duties[19]. Such regulation puts an additional bureaucratic burden on these public subjects and the General Inspector[20]. In our opinion, this provision has both positive and negative effect. On the one hand, one may claim that thanks to such provision one institution exercises a full control over protection of personal data. On the other hand, it multiplies duties of the General Inspector, since those institutions are authorized by law to collect and transfer personal data. Currently, the need to register a data filing system is less clear than 10 years ago when the Law entered into force. Importantly, Directive 95/46/EC does not entail the registration obligation of the data controllers.

[38]. Another uncertainty concerns exclusion of the obligation to inform the data subject[21] and to authorize processing of sensitive data without the consent of the

[18] Art. 2 para. 2: 'The Act shall apply to the processing of personal data in: 1) files, indexes, books, lists and other registers, 2) computer systems, also in case where data are processed outside from a data filing system'.

[19] Judgment of the Regional Administrative Court in Warsaw affirming the duty to register the manual register of complaints and petitions addressed to Regional Prosecutor's Office, WSA II SA/Wa 734/05

[20] Compare the discussion on this subject at: http://prawo.vagla.pl/node/7653

[21] Art. 25 para. 2: The duty to inform the data subject does not apply if "the provision of other law provides or allows for personal data collection without the need to notify the data subject".

data subject[22] if other statute provides so. Instead of such a general and rather broad clause referring to other statutes, Directive 95/46/EC describes specific situations in an exhaustive list. The Directive permits restriction of the duty to inform the data subject only on the account of important public interests listed therein. Likewise only a substantial public interest can justify restriction of rights of data subjects – by adoption of a legal norm or decision of the supervising authority - concerning protection of their sensitive data.

[39]. According to the Directive, Member States shall ensure that persons who suffered damage as a result of an unlawful processing operation or as a result of any act incompatible with the national provisions with respect to data protection receives compensation from the controller for the damage suffered. The Data Protection Law does not provide for such liability. Such person may claim civil liability or tort liability under relevant provisions of the Civil Code. In case when the data subject claims violation of personal rights pursuant to Art. 23 and 24 of Civil Code, the administrator of data filing system would have to prove that processing of data did not constitute an unlawful action. The lawfulness of processing will be established if the data subject agreed for it or if the controller acted in accordance to the law.

[40]. However, violation of personal data protected under the Data Protection Law does not have to constitute a breach of personal rights pursuant to Art. 23 and 24 of Civil Code[23] or the rules of unfair competition. Provisions on protection of personal rights provide for the possibility to sue when personal right of an individual is violated (e.g. honor, good name, privacy etc.) and this violation is illegal. In such a case an individual may claim apologies, damages or paying a certain sum of money to social benefit purpose. Rules on unfair competition provide for a possibility to sue a competitor (other business entity), when it commits an unfair competition action (e.g. by using trademarks without consent, by selling fake products, by using database of clients of one business entity without a permission). In such a case, a business entity may claim damages, apologies and also different restitution actions (e.g. destroying all materials produced in violation of unfair competition rules). Another possibility is to invoke tort liability pursuant to Art. 413 of Civil Code. This provision is a general provision establishing tort liability for any actions violating somebody's

[22] Art. 27 para 2: Processing of sensitive data is possible if "the specific provisions of other statute provide for the processing of such data without the data subject's consent and provide for adequate safeguards"

[23] In 2000 the Regional Court in Łódź ruled that sending Christmas cards to prospective clients of a bank in spite of the fact that they disagreed to processing of their personal data constituted a breach of right of privacy and awarded the party 20 000 PLN damage for violation of Art 23 and 24 of Civil Code. However, such finding does not seem to be well-founded. Rather there has been a viola(Number of judgment and the exact date is not known to the authors of this report. It was referred to in the commentary to the Law – J. Barta et all, supra note 13).

else rights. There is only a requirement to show causality between unlawful processing of personal data, material damage suffered by the data subject and the fault of a person / institution responsible to protect personal data. [see more in Chapter IV para 137].

[41]. Under the Data Protection Law, the consent to process personal data cannot be withdrawn. It seems that taking the perspective of consumer protection, the inclusion of a provision enabling the data subjects to withdraw their consent or to give consent for a limited time would be advised. However, the business representatives taking part in social consultations concerning the draft law introducing the institution of a withdrawal claim that it will endanger the security of business transactions and generate additional costs.

1.4. Data protection in electronic communication

[42]. In July 2004, Poland adopted the Telecommunication Law[24], which implements Directive 2002/58/EC on privacy and electronic communications[25]. The same Directive has been also implemented in the Law on Provision of Services by Electronic Means[26]. The latter does not apply to provision of telecommunication services in order to avoid doubling-up regulation of the same subject matter. In general, the Telecommunication Law contains higher standard of data protection, thus it excludes application of the Data Protection Law. However, in some parts it is not clear which law presents a higher standard since they use different concepts of data protection. In any case, the controllers of data filing systems within the telecommunication sector fall under obligations established in Chapter V of the Data Protection Law.

[43]. The Telecommunication Law defines telecommunication secrets not only through reference to the content of transmission, but also to data about users of telecommunication services. In the light of its provisions, transmission data, localization data and information about trials to obtain connection may constitute an individual's personal data.

---

[24] Telecommunication Law of 16.07.2004, *Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, Dziennik Ustaw* [Journal of Laws], No 171, Item 1800, as amended.

[25] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) , Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

[26] The Law of 18.07.2002 on Provision of Services by Electronic Means, *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*. Journal of Laws [*Dziennik Ustaw*] of 2002 No 144, Item 1294, as amended. The Law in one part implements the Directive 200/31/EG on E-Commenrce, as well as Directive 2002/58/EG on privacy and electronic communication.

[44]. The Telecommunication Law introduces a general prohibition of making oneself familiar with the content or data covered by the telecommunication secrets, as well as recording, storing, forwarding or using such content or data. There are, however, several exceptions.

[45]. The Telecommunication Law specifies so-called permanent data [*dane stałe*] of an individual being a user of publicly available telecommunication services, which are collected for conclusion of the contract. The processing of such data is based on the provisions of the Telecommunication Law. Therefore, no consent of the data subject is required. Other personal data can be processed only after the consent has been given. The Telecommunication Law regulates also specifically the processing of transmission and localization data, as well as publication of subscribers' lists. Since 2000, the inclusion into the subscribers' list is not automatic, but requires individual consent of an individual that can be withdrawn any time. The consent is, however, not required from other – than individuals – persons, unless it threatens vital interest of such persons. Problems may arise when, for example, the entrepreneur is a natural person.

[46]. The Telecommunication Law regulates also the issue of data retention following Directive 2006/24/EC on the data retention[27]. The Telecommunication Law stipulates the duty of the operators of public telecommunication network or providers of publicly available telecommunication service processing transmission data of subscribers and end users to retain such data for the period of 2 years in order to enable specific state organs to fulfill tasks and duties in the area of defense, security of the state and public safety and order. After this period, the data are removed or made anonymous.

[47]. With respect to the Law on Provision of Services by Electronic Means, it grants the protection of personal data irrespectively of the fact whether they are processed in a data filing system of outside it. Thus, it refers to the 15th Recital of Directive 95/46/EC expanding the protection to such cases when data are automated or when they are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals. However the relevant provisions of the Data Protection Law apply as well to cases when data are processed within the filing system for the purpose of provision of electronic services. Characteristically, the Law on Provision of Services by Electronic Means foresees explicitly withdrawal of the consent where processing is based upon it. This Law contains different rules for processing different types of data (permanent, exploitation and financial data).

[27] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 002/58/EC, *Official Journal L 105 , 13/04/2006 P. 0054 – 0063*.

2. Data Protection Authority

2.1. General Information on the General Inspector for Protection of Personal Data

[48]. *Generalny Inspektor Ochrony Danych Osobowych (GIODO)* [General Inspector for the Protection of Personal Data] is a body responsible for the protection of personal data. There is no direct reference to the General Inspector in the Polish Constitution. Articles 47 and 51 of the Constitution (referred to in Chapter 1) only indirectly govern the scope of the General Inspector's authority.

[49]. Under the Data Protection Law, the General Inspector is appointed and dismissed by the Sejm with consent of the Senate. The General Inspector's term of office is four years. The same person may be reappointed only twice.

[50]. At the request of the General Inspector, the *Marszałek* [Speaker] of the Sejm appoints a deputy General Inspector.

[51]. The legal powers of the General Inspector are specified in the Data Protection Law. In accordance with the Data Protection Law, the General Inspector has the right to:

- supervise the compliance of data processing with the Data Protection Law and other laws in this matter;
- issue administrative decisions and investigate complaints with respect to the enforcement of the personal data protection laws;
- keep the register of data filing systems and provide information on the registered data files;
- issue opinions on draft statutes and ordinances with respect to personal data protection,
- initiate and undertake activities to improve personal data protection,
- participate in the work of international organisations and institutions involved in personal data protection.

[52]. If the data protection regulations are infringed, the General Inspector, acting ex officio or on a motion of the interested person, orders, by means of an administrative decision, the restoration of the proper legal state, and in particular to:

- remedy the defect,
- complete, update, correct, disclose or not to disclose personal data,
- apply additional measures protecting the collected personal data,
- suspend any transfer of personal data to a third party state,
- safeguard the data or to transfer them to other entities,
- erase the personal data.

[53]. If the General Inspector finds that any action or omission of the head of an organisational unit, the employee of an organisational unit or other individual performing the function of a data administrator satisfies the criteria of a statutory offence, the General Inspector will report such an offence to the law enforcement authorities, enclosing any evidence documenting the suspicion that a crime has been committed.

[54]. The General Inspector acts on the basis of the Code of Administrative Procedure[28], subject to any regulations of the Data Protection Law providing for any contrary procedures.

[55]. The General Inspector has also to follow certain pieces of secondary legislation to the Data Protection Law[29], as well as internal regulations applying to its work.[30]

[56]. The General Inspector performs his/her duties assisted by the Office of the General Inspector (*Biuro Generalnego Inspektora Ochrony Danych*

[28] Code of the Administrative Procedure of 14 June 1960, *Ustawa z dnia 14 czerwca 1960 r.- Kodeks postępowania administracyjnego*, the uniform text in the Journal of Laws [*Dziennik Ustaw*] of 2002, No. 98, Item 1071, as amended) .

[29] The Ordinance of the President of the Republic of Poland of 3 November 2006 on granting the Statute to the Office of the General Inspector for the Protection of Personal Data (Journal of Laws No. 203, item 1494); the Ordinance of the Minister of Interior and Administration of 29 April 2004 on the documentation of processing the personal data and technical and organisational conditions applicable to the IT systems and devices designed for processing the personal data (Journal of Laws, No. 100, item 1024); the Ordinance of the Minister of Interior and Administration of 29 April 2004 on the specimen of the data registration filing document to be submitted to the General Inspector for the Protection of Personal Data (Journal of Laws, No. 100, item 1024), and the Ordinance of the Minister of Interior and Administration of 22 April 2004 on the specimen of the personal authorisation and service identity card of an inspector of the Office of the General Inspector for the Protection of Personal Data (Journal of Laws, No. 94, item 924).

[30] The Internal Regulation [*Zarządzenie*] No. 29/2007 of the General Inspector for the Protection of Personal Data introducing the Organisational Regulations of the General Inspector Office; the Annex to the Internal Regulation No. 29/2007: Organisational Regulations of the General Inspector Office.

Osobowych) headed by the Office Director. The Office of the General Inspector is composed of the following departments:

- Jurisdiction, Legislation and Complaints Department (staff: 25 persons);
- Inspection Department (20);
- Personal Data Filing Systems Registration Department (14);
- Social Education and International Co-operation Department (10);
- IT Department (14);
- Organisational and Administrative Department (15);[31]

[57]. The last two departments perform support functions for the Office of the General Inspector and do not deal with performance of statutory competences.

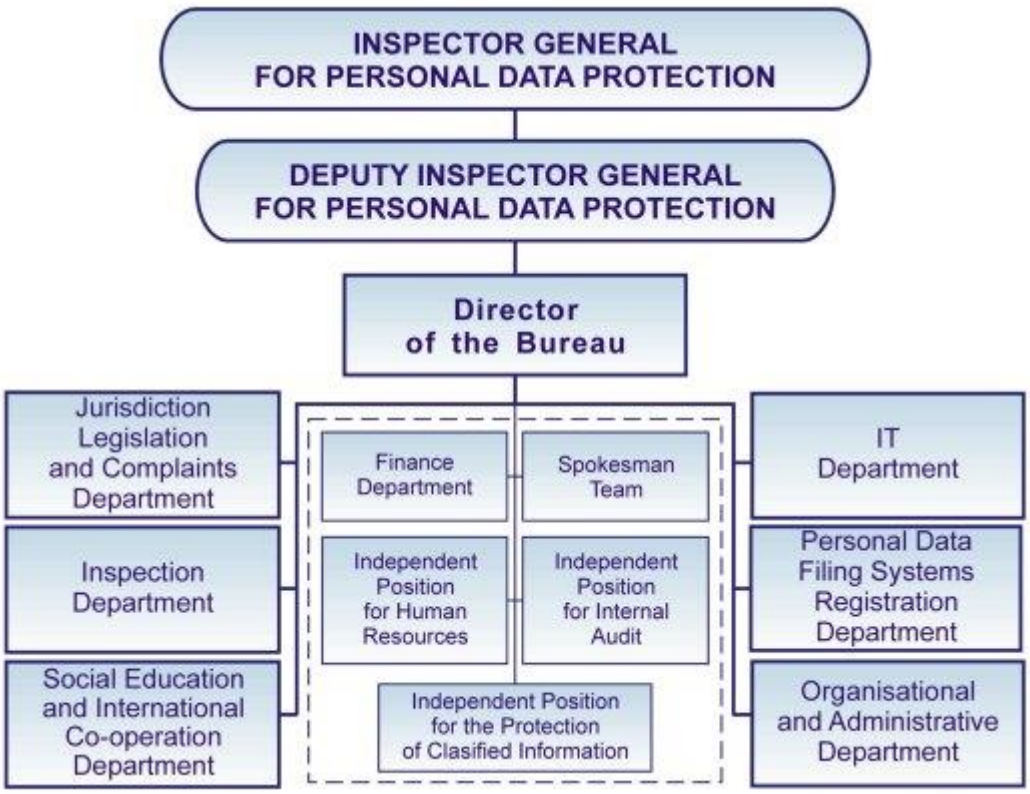
[58]. The following are the main tasks of the Jurisdiction, Legislation and Complaints Department: answering the clients' questions regarding personal data protection legislation, issuing opinions on bills and draft regulations concerning personal data protection, participating in legislative works, conducting administrative proceedings in respect of the enforcement of personal data protection laws, preparing draft offence reports and motions to initiate disciplinary action.

[59]. The Inspection Department's primary tasks include: controlling the compliance of personal data processing with applicable law, initiating and conducting administrative proceedings in response to any defects established during the inspection, drafting schedules of planned inspections.

[60]. The main objectives of the Personal Data Filing Systems Registration Department are to collect and register data filing systems, entering information into the national, publicly available register of data filing systems and create registry documents for the filed systems, prepare drafts of intervention statements regarding the obligation to register.

[61]. The actions performed by the Social Education and International Co-operation Department consist primarily in promoting the knowledge of personal data, organising and carrying out educational activities, considering applications for transfer of the personal data to third party countries as well as conducting comparative legal studies of the international law instruments and individual domestic regulations concerning the protection of personal data.

[31] Data on staff has been taken from The *2007 General Inspector Operations Report*, p. 6, available at www.giodo.gov.pl.



[62]. The General Inspector budget for 2008 was PLN 13,717,000 (approx. 3.25m EUR).[32]

[63]. At the end of December 2007, the General Inspector Office was staffed with 117 full-time employees, including 103 principal specialists and 17 members of the support personnel. Out of 97 employees with a university degree, 67 were lawyers.[33].

[32] The Draft 2008 Budget of the Inspector General for the Protection of Personal Data (available at www.giodo.gov.pl).

[33] The *2007 General Inspector Operations Report*, p. 6, available at www.giodo.gov.pl.

2.2. Powers of the General Inspector in the light of the Directive 95/46/EC

[64]. Pursuant to Article 28(2) of the Directive 95/46/EC, a Member State must provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. From the formal standpoint, the said obligation has been fulfilled by the provisions of Article 12 of the Data Protection Law. It provides that the General Inspector's tasks include 'issuing opinions on bills and draft regulations with respect to personal data protection' (subsection 4).

[65]. Unfortunately, the Data Protection Law fails to introduce any general duty to notify the General Inspector of relevant legal acts being prepared by the state authorities responsible for the legislative process. In consequence, the General Inspector is consulted on draft legislation only if a state entity preparing legislation so decides. It means that in most instances that the General Inspector is consulted where the subject-matter of the proposed legislation directly relates to the subject of the personal data protection.

[66]. However, there are also pieces of draft legislation which contain provisions putting, even marginally, some limitations on privacy. Such legal acts are usually not consulted by the General Inspector. Because of the vast number of the proposed legal acts of various levels, the General Inspector's ability to monitor the current legislative works is virtually non-existent. Therefore, the actual implementation of the said statutory provision leaves much to be desired. Also, the General Inspector's opinion expressed during the consultations is treated solely as an advisory voice of an administrative body (alike a voice of a Ministry) which may be left unheard. Accordingly, the General Inspector in the process of consultation of draft legislation acts more like one of stakeholders, but not as an institution which has a stronger voice in matters having impact on data protection. Therefore, the opinions in question are not deemed to be issued by an independent body which has a right to interpret the Constitution. In our opinion it is a problem. We draw this conclusion by comparing opinions of the General Inspector with opinions of the Office of the Committee for the European Integration [*Urząd Komitetu Integracji Europejskiej*]. Opinions of the latter have a direct impact on the legislation and draft regulations are amended when the Office claims they are contrary to EC law. We do not claim that the General Inspector's opinions should always trump over opinions of other bodies (or drafters of regulations). We claim that institutionally they should have a higher status than a typical consultation on draft law and should be more seriously taken into account. Please note that non-taking into account poses then a risk of serious violation of law and rights of individuals.

[67]. In accordance with Article 28(3) of the Directive 95/46/EC, a supervisory authority must be equipped with investigative and intervention powers. In this respect, the Data Protection Law sets out a detailed list of the powers conferred upon the General Inspector and General Inspector's controllers (inspectors).

[68]. Article 14 of the Data Protection Law permits controllers to enter, between 6 a.m. and 10 p.m. and upon producing a personal authorisation and a service identity card, any premises on which a data system is located and conduct necessary examination or other control activities to assess the compliance of the data processing with law. Further, controllers may demand explanations and summon and interview any person, to the extent necessary to determine the actual state of affairs. They may also review any documents and data directly related to the subject-matter of the inspection and make copies thereof, as well as inspect any devices, carriers and IT systems designed for data processing and commission expert reports and opinions. Consequently, a head of the inspected organisational unit and the controlled individual who performs the function of a personal data administrator are legally required to enable the inspector to perform the inspection.[34]

[69]. If the personal data protection regulations are infringed, the General Inspector, acting *ex officio* or upon a motion of an interested person, orders, by means of an administrative decision, to bring the situation into compliance with law. In particular, it may require to remedy defects in protection of personal data, supplement, update, correct the personal data, apply additional measures protecting the personal data, suspend the transfer of personal data abroad, safeguard the data or transfer them to other entities or erase the personal data.[35]

[70]. Basing on the conclusions of the inspection, it is possible to start disciplinary action and/or other legal proceedings against the persons liable for defects and request that he/she be informed on the results of such proceedings and any measures applied.[36]

[71]. If the General Inspector finds that any action or omission of the head of an organisational unit, an employee of an organisational unit or other individual performing the function of a data administrator satisfies the criteria of a statutory offence, the General Inspector will report such an offence to the law enforcement authorities, enclosing any evidence documenting the suspicion that a crime has been committed.[37]

[72]. In our opinion such powers are being appropriately exercised and the General Inspector does not face any impediments regarding realisation thereof. We base

[34] Cf. Article 15 of the Act.
[35] Cf. Article 18 of the Act.
[36] Cf. Article 17(2) of the Act.
[37] Cf. Article 19 of the Act.

this opinion on our review of the annual reports of the General Inspector and general observation of its activities. The only limitations in this respect are staffing and financial capabilities of the General Inspector and lack of law enforcement authorities' understanding for the reports on the offences allegedly committed, submitted by the Inspector. Pursuant to the provisions of the Criminal Procedure Code[38], the General Inspector has no right to appeal against a refusal to prosecute the offences being a violation of the Data Protection Law. In consequence of that fact (and a relatively low social awareness of the criminal provisions included to the Data Protection Law), a significant part of the General Inspector's reports submitted to the prosecution service is virtually ignored as the General Inspector is unable to argue the case before the court.

[73]. Being aware of ineffectiveness of such an instrument, the General Inspector relatively seldom reports the infringements to the law enforcement authorities. Despite the fact that motions to prosecute the offences submitted to the prosecution service are well-prepared and contain all required details, the vast majority of them tend to be dismissed. For example, in 2007, out of 36 motions to prosecute submitted by the General Inspector only five resulted in indictment brought before the court by the prosecution authorities.[39] In our opinion this practice results from a general practice of the prosecution authorities and approach to non-typical cases and is not strictly connected with the protection of personal data. Prosecution authorities are not effective in Poland and there is a general claim that many decisions are not issued following careful examination (e.g. refusals to start investigation), but purely because of lack of personal capabilities or lack of sufficient supervision over prosecution and its decisions. It is a general problem and in our opinion one of the most important deficiencies of the whole Polish justice system. Therefore, prosecution authorities strongly await the complex reform.

[74]. At the same time, the General Inspector experiences no hindrances in examining the complaints received from individuals, business entities and institutions.

[75]. Taking into account above findings, it seems appropriate to establish a General Inspector's duty to issue an opinion on each and every statutory legal act and regulation, which would ensure that no provision potentially infringing the protection of information are left unnoticed by the Inspector. Such an enhanced scope of the General Inspector's obligations should be probably reflected by an increased financing awarded to the Office of the General Inspector. The General Inspector draft budget is prepared by the General Inspector itself and attached,

[38] Code of Criminal Proceedings of 6 June 1997, *ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego*, Journal of Laws (*Dziennik Ustaw*) of 1997, No. 89, item 555, as amended.

[39] Annex 5 to the *2007 General Inspector Operations Report*, p. 161, available at www.giodo.gov.pl.

without anybody's interference, to a state draft budget for the next year. Obviously, financial status of the state represented by the Ministry of Finance compels the General Inspector to self-limit the spending plans.

[76]. Furthermore, the General Inspector plays only an advisory role in the legislation process. Its constitutional position is not strong enough to guarantee that the Inspector's arguments will always prevail in dealings with the legislative bodies. Moreover, the General Inspector has no right to challenge unconstitutional laws before the *Trybunał Konstytucyjny* (*TK*) [Constitutinal Tribunal, CC], even in matters regarding the protection of information and personal data, which additionally weakens its position within the legislative process. The General Inspector may only, alike every citizen or institution, request that such a complaint be brought by the *Rzecznik Praw Obywatelskich* (RPO) [Commissioner for Civil Rights Protection, hereinafter referred to as the **"Ombudsman"**] or other authorized institution by virtue of Article 188 of the Constitution. However, since the relations between the General Inspector and the Ombudsman are quite tense (e.g. due to a certain competition existing between the two bodies in the area of the protection of civil rights), the former cannot count on an efficient co-operation with the latter. Please note that the Ombudsman infers its competence to act from a general competence to deal with citizens' rights and freedoms. It has also more competences to act in certain areas (e.g. to challenge constitutionality of law). Furthermore, it is a constitutional organ (it has a regulation in the Constitution of Poland), while the General Inspector does not have. In summary, it seems justified to give the General Inspector the powers it lacks today and improve its constitutional position by enshrining its authority in the Constitution of the Republic of Poland. There are more and more discussions in Poland on amending the Constitution. It may happen that strengthening of position of the General Inspector will be one of the amendments. Current situation (and competition between Ombudsman and the General Inspector) is not a deficiency of the system, since it does not cause serious problems. However, in order to avoid them in a future and to strengthen the General Inspector some reforms should be done.

[77]. With reference to the issue of the authorities ignoring the General Inspector's reports on offences, it may be proposed either to amend the Criminal Procedure Code (granting the General Inspector the right to appeal against a prosecutor's decision refusing to prosecute the alleged offence) or to abandon the right to initiate a criminal action altogether, giving the Inspector the power to impose penal and administrative means (fines), maintaining at the same time currently existing possibility to bring an appeal against its decision before an administrative court.

2.3. Remit

[78]. The tasks of the General Inspector include supervising the compliance of data processing with the personal data protection laws. However, the Act excludes the possibility of carrying out such supervisory actions against certain categories of institutions. The latter are e.g. the administrators of the data classified as the state secrets due to the requirements of defence and security of the state, protection of human life and health, protection of property or public safety and order as well as the administrators of the data concerning persons being the members of a church or other religious organisations with an established legal status, processed for the purposes of such a church or religious organisation.

[79]. Moreover, the Act excludes a possibility to take the majority of the General Inspector's actions towards the administrators of the data which have been obtained as a result of the operational and investigative activities conducted by the officers of the agencies authorised to perform such activities[40]. The only action that may the General Inspector take in order to verify the above-mentioned administrators' compliance with the Data Protection Law is to submit a query.[41] However, the General Inspector has no authority to enforce an appropriate conduct of the administrator or even to demand a satisfactory response to its own query. Such limitations to the General Inspector's powers are insufficiently justified by the guaranties of maintaining other values.

2.4. Allocation of resources *vis-à-vis* effectiveness of GIODO

[80]. The budget and staffing of the General Inspector Office seems to be adequate for the purposes of implementation of tasks conferred upon the General Inspector. On the other hand, due to insufficient awareness of the significance of the personal data protection amongst the public and public officials, the General Inspector is often forced to allocate its funding to the purposes falling beyond its statutory duties, e.g. in order to disseminate the information on the rights of the citizenry (the informational campaign regarding Poland's accession

[40] In particular processed by the *Agencja Bezpieczeństwa Wewnętrznego (ABW)* [Internal Security Agency, ISA], *Agencję Wywiadu (AW)* [Foreign Intelligence Agency, FIA], *Służba Kontrwywiadu Wojskowego (SKW)* [Military Counter-intelligence Service, MCS], *Służba Wywiadu Wojskowego (SWW)* [Military Intelligence Service, MIS] and *Centralne Biuro Antykorupcyjne (CBA)* [Central Anticorruption Bureau, CAB].

[41] Cf. Article 43 of the Act.

to the Schengen Agreement and resulting consequences for the flow and security of information).[42]

[81]. Furthermore, an increase of the General Inspector budget could possibly result in a significant enhancement of its competences in respect of the personal data protection. Such enhancement - in light of the lack of understanding of the subject by the state authorities - would be a value impossible to overestimate.

[82]. In conclusion, the budget and staff of the General Inspector are sufficient in relation to the powers conferred upon the General Inspector, but the powers themselves are too narrow relative to the needs. It must be noted that entrenching the General Inspector's position in the Constitution would definitely improve the ability to prepare the institution's budget in more advantageous manner.

2.5. Guarantees of independence

[83]. Statutory guarantees of General Inspector's independence primarily pertain to the formal aspect of its Office's activities. Under Article 8 of the Data Protection Law, the General Inspector is appointed and dismissed by the Sejm of the Republic of Poland with consent of the Senate. An individual is eligible for the appointment to the office of the General Inspector provided that he/she is a Polish citizen and has a permanent residence in the Republic of Poland, is of the highest moral standing, has a university degree in law and relevant professional experience and has no criminal record**.**

[84]. Formally, General Inspector's independence is guaranteed by the provision which states that performance of its tasks is governed solely by the statutory provisions**.** The General Inspector can be reappointed only once. The General Inspector term of office expires at the moment of his/her death, dismissal or loss of the Polish citizenship. The Sejm, acting upon the consent of the Senate, may dismiss the General Inspector only if he/she has withdrawn from the office, become permanently incapacitated due to a disease, violated the affirmation made or has been convicted for committing an offence by virtue of a final court judgment. Comparing to other institutions, such grounds for dismissal establish a pretty high standard of independence, as it is quite difficult to dismiss the General Inspector due to typical political reasons.

[85]. The General Inspector also enjoys legal immunity.[43]

[42] The *2007 General Inspector Operations Report*, p. 103, 104, 106, available at www.giodo.gov.pl.

[43] Cf. Article 11 of the Act.

[86]. Article 10 of the Data Protection Law forbids the General Inspector to assume any other position (except for the post of a university professor) and to perform any other professional activities. Accordingly, this provision guarantees the General Inspector's independence from other entities. Furthermore, the General Inspector may not be a member of any political party, trade union and carry out any public activity inconsistent with the dignity of his/her office.

[87]. Nevertheless, the real independence of the General Inspector is greatly limited. It is a consequence of the weak constitutional position mentioned above and, in particular, no constitutional grounding for the Inspector's activities. Consequently, other state bodies treat the General Inspector as yet another 'regular' administrative body, rather than the actually independent and significant entity.

[88]. The General Inspector office was established in 1998. That year Ewa Kulesza, *LL. D.*, was elected the first General Inspector and reappointed in 2002. Since July 2006, the post has been held by Michał Serzycki (a lawyer).

2.6. Activity

[89]. In 2007, the General Inspector, at his own initiative, conducted 167 personal data processing inspections, including 40 in the public administration bodies, 29 in banks and other financial institutions, 29 in entities rendering health care services, pharmacies, organisational units of the professional self-government of physicians and dental practitioners and the organisational units of the *Zespół Ubezpieczeń Społecznych* (ZUS) [the Social Insurance Institution, SII], archives and other entities.[44]

[90]. Out of 781 administrative decisions issued by the General Inspector in 2007, 130 resulted from the inspections conducted by the General Inspector on his own initiative.[45]

[91]. In 2007, the General Inspector submitted 26 formal addresses to the state bodies, including central government authorities.[46] We have not studied exact result of each of these addresses. However, most of them were taken into account in further actions of authorities.

[44] The *2007 General Inspector Operations Report*, p. 10-21, available at www.giodo.gov.pl.
[45] The *2007 General Inspector Operations Report*, p. 22, available at www.giodo.gov.pl.
[46] Annex 1 to the *2007 General Inspector Operations Report*, p. 136-139, available at www.giodo.gov.pl.

2.7. Monitoring

[92]. For the General Inspector, the basic sources of knowledge on violations of the provisions concerning personal data protection are citizens' complaints and inspections conducted by the General Inspector. The former generates more information than the latter. In 2007, 796 complaints were filed with the Jurisdiction, Legislation and Complaints Department, whereas, as already mentioned, the General Inspector conducted 167 inspections on his own initiative. It seems therefore that the General Inspector was not particularly active in taking actions on his own initiative.

2.8. Availability of decisions and reporting

[93]. All decisions issued by the General Inspector and some of the addresses are available at the website: www.giodo.gov.pl. The General Inspector's decisions are broken down according to their subjects (institutions being addressees of the decisions) and substance (subject-matter which the interventions concerned). In addition, the Annual Reports are published, in which the key General Inspector's interventions and addresses are broadly discussed, accompanied by the annexed lists of those actions.

[94]. Every annual report comprises of an introduction – setting out the legal basis of the General Inspector's actions, as well as the staff number and budget implementation information, a comprehensive analytical part, the second part – specifying the nature of the General Inspector's activity in a given year, the third part – containing conclusions and the General Inspector's policy for subsequent periods, as well as the annexes. In total, the report has about 150-170 pages.

[95]. The analytical part of the report is divided into sections, in accordance with the General Inspector's scope of activities. It describes inspection and administrative activities taken by General Inspector in a given year as well as the maintenance of the personal data systems register and information provided in this respect. The part in question contains also information on issuing the General Inspector's opinions on bills and draft regulations and the office's informational activity as well as its actions regarding the interpretation of laws.

[96]. The annex to the annual report includes lists naming various actions taken by the General Inspector: general addresses, addresses submitted to the legal entities, inspections, training courses. The decisions issued by the *Najwyższy Sąd Administracyjny* (NSA) [The Supreme Administrative Court, SAC] and the

Wojewódzkie Sądy Administracyjne (WSA) [Provincial Administrative Courts, PACs] in matters handled by General Inspector are listed separately.

[97]. Moreover, the General Inspector's publications and key judicial decisions concerning the matters of the personal data protection are available at the General Inspector's website.

2.9. Working Group Article 29

[98]. The General Inspector participates actively in the works of the Article 29 Working Group; the reports from the Group's sessions and resolutions adopted can be found at the General Inspector's website. They are systematically translated into Polish. Certainly, the General Inspector takes account of the Article 29 Working Group's resolutions. When they are relevant to the given subject matter they are used to justify decisions issued by the General Inspector, opinions and addresses. For example, Article 47 and 51 of the Polish Constitution are interpreted taking into account opinions of the Working Group Article 29. However, the General Inspector's relatively weak position in the legislative process and the process of the judicial review process renders the Inspector's efforts to interpret the laws of Poland in line with the Group's resolutions quite ineffective.

2.10. Advisory role

[99]. As already mentioned above, the General Inspector is treated in the legislative process as a 'regular' central administration body and, consequently, the General Inspector's conclusions and opinions are considered to be an advisory voice rather than a voice of an independent institution. Nevertheless, in 2007 348 statutes were submitted to the General Inspector to be reviewed in respect of their compliance with the personal data protection laws. The General Inspector's arguments often prevented implementation of the provisions violating the Act on the Protection of Personal Data.[47]

[47] For instance, the General Inspector opposed the introduction of certain provisions of the draft regulation of the Minister of Finance on the detailed scope of processing the information regarding individuals after the expiration of an obligation under an agreement entered into with a bank or other financial institution with a statutory authorisation to grant loans and the procedure for removal of such information (2007 Journal of Laws No. 56, item 373), establishing too long (12-year) period for keeping the personal data. The Inspector's opposition has been accepted.

2.11. Awareness raising role

[100]. Due to low legal awareness in respect of personal data protection, one of the General Inspector's key tasks is to increase both the citizens' and public officials' knowledge on this subject. The General Inspector is fully aware of that need. Therefore, educational and advocacy activities constituted a major part of the office's actions.

[101]. In 2007, the General Inspector conducted 60 training courses for civil servants and officials of different levels of administration and branches of government (ministries, self-governmental units, judges, curators, etc.).

[102]. The Office of the General Inspector organised academic conferences, disseminating information about the General Inspector and the personal data protection system.[48] It cooperated with the press, including mass-edition nationwide press covering the issues connected to the right to privacy (e.g. the series of discussion in *Gazeta Prawna* (leading daily on legal issues) and *Gazeta Wyborcza* (leading daily newspaper with general content). Working together with the *Wydawnictwo Sejmowe* [The Sejm Publishing House], the General Inspector prepared 5 publications introducing the theme of the protection of data and information.[49] The office held the internship programme for law students. Furthermore, the Office of the General Inspector offered advice by telephone, post (1298 cases in 2007) and electronically in respect of the principles of registering personal data systems. The General Inspector also disseminates information on the personal data protection by organising conferences[50] and training courses for students in cooperation with higher education institutions.[51]

[48] For instance, the conference held in the General Inspector's head office titled '*Czy nasze dane są bezpieczne w Systemie Informacyjnym Schengen?*' [Are our Data Safe in the Schengen Information system?] (17 December 2007); the conference on illegal practices of marketing companies '*Wygrałeś? – Uważaj!' [You have won? Beware!*] (4 April 2007).

[49] A series of publications is named as "ABC of Personal Data" and includes five specific publications. They are available in the catalogue of Wydawnictwo Sejmowe under the following link: http://wydawnictwo.sejm.gov.pl/serie/abc_danych_osobowych.html

[50] E.g. the General Inspector held the conference '*Ochrona danych osobowych – gwarancja czy zagrożenie prywatności'* [Personal Data Protection - a Guarantee or a Threat to the Privacy] at the Koźmiński Univeristy in Warsaw (27 January 2007).

[51] E.g. the College of Finance and Business Administration in Gdańsk, Cardinal Stefan Wyszyński University, Leon Koźmiński University in Warsaw.

3. Compliance

[103]. According to the Data Protection Law every entity performing the processing of data is obliged to register a data filing system to registration by the General Inspector[52]. The registration may be completed by filling a special form directly in the General Inspector office or through Internet (the General Inspector web page).

[104]. The registration form, concerning the data filing system submitted to the registration, should contain the following[53]:

- an application for entering the personal data filing system into the register of filing systems,
- an indication of the entity running the filing system and the address of its seat or place of residence, including the identification number in the register of enterprises setting up in business, if applicable, and the legal grounds on which he/she is authorised to run the data filing system, and in case of the entity have its seat in a third country, indication of this subject and the address of its seat or place of residence,
- the purpose of the processing of data,
- description of the categories of data subjects and the scope of the processed data,
- information on the ways and means of data collection and disclosure,
- information on the recipients or categories of recipients to whom the data may be transferred,
- the description of technical and organisational measures applied for assuring the security of processed data,
- information on the ways and means of fulfilling technical and organisational conditions of data storing (also computer systems and all sorts of devises enabling the data storing),
- information relating to a possible data transfer to a third country.

[105]. The data filling system is defined by the Data Protection Law as "any structured set of personal data which are accessible pursuant to specific criteria, whether centralised, decentralised or dispersed on a functional basis".[54]

[52] Art. 40 of the Act.
[53] Requirements provided in art. 41 of the Act.

[106]. There is no obligation of registration of data processing for the entities processing data which:

- constitute a state secret due to the reasons of state defence or security, protection of human life and health, property, security, or public order,
- were collected as a result of inquiry procedures held by officers of the bodies authorized to conduct such inquiries (e.g. prosecutors),
- are processed by relevant bodies for the purpose of court proceedings and on the basis of the provisions on National Criminal Register,
- are processed by the General Inspector of Financial Information,
- relate to the members of churches or other religious unions with an established legal status, being processed for the purposes of these churches or religious unions,
- are processed in connection with the employment by the controller or providing services for the controller on the grounds of civil law contracts, and also refer to the controller's members and trainees,
- refer to the persons availing themselves of their health care services, notaries or legal advice, patent agent, tax consultant or auditor services,
- are created on the basis of electoral regulations,
- refer to persons deprived of freedom,
- are processed for the purpose of issuing an invoice, a bill or for accounting purposes,
- are publicly available,
- are processed to prepare a thesis required to graduate from a university or be granted a degree,
- are processed with regard to minor current everyday affairs[55].

[107]. The General Inspector has limited investigatory powers on data processed by special state services (like e.g. intelligence services).[56]

[108]. Even when an entity processing data is not obliged to register the processing of data, it still needs to fulfil the requirements enabling the processing of data (e.g. the data subject has given his/her consent, processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision etc.). The entity is also required to provide to the subject data information about its

[54] Art. 7 point 1 of the Act.
[55] Art. 43 par. 1 of the Act.
[56] Art. 43 par. 2 of the Act.

seat, address, source of data, the existence of the data subject's right of access to his/her data and the right to rectify these data and many others[57].

[109]. Furthermore, the entity performing the processing of data should protect the interests of data subjects with due care, and in particular to ensure that the data are processed lawfully, the data are collected for specified and legitimate purposes and no further processed in a way incompatible with the intended purposes, the data are relevant and adequate to the purposes for which they are processed and that the data are kept in a form which permits identification of the data subjects no longer than it is necessary for the purposes for which they are processed[58].

[110]. After lodging a registration form with the General Inspector the entity may demand a registration confirmation issued by the General Inspector office. The entity has to pay 17 PLN (approx. 4.25 EURO) of stamp duty in order to receive such a confirmation.

[111]. The processing of sensitive data as a general rule is prohibited[59]. The processing of sensitive data is allowed only when:

- the data subject has given his/her written consent, unless the processing consists in erasure of personal data,
- the specific provisions of other statute provide for the processing of such data without the data subject's consent and provide for adequate safeguards,
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent until the establishing of a guardian or a curator,
- processing is necessary for the purposes of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non-profit-seeking organisations or institutions with a political, scientific, religious, philosophical, or trade-union aim and provided that the processing relates solely to the members of those organisations or institutions or to the persons who have a regular contact with them in connection with their activity and subject to providing appropriate safeguards of the processed data,
- processing relates to the data necessary to pursue a legal claim,
- processing is necessary for the purposes of carrying out the obligations of the controller with regard to employment of his/her employees and other persons, and the scope of processing is provided by the law,

[57] The obligations are provided in art. 24 and 25 of the Act.
[58] Art. 26 par. 1 of the Act.
[59] Art. 27 par. 1 of the Act.

- processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards,
- the processing relates to those data which were made publicly available by the data subject,
- it is necessary to conduct scientific researches including preparations of a thesis required for graduating from university or receiving a degree; any results of scientific researches shall not be published in a way which allows identifying data subjects,
- data processing is conducted by a party to exercise the rights and duties resulting from decisions issued in court or administrative proceedings[60].

[112]. In practice, regular inspections performed by the General Inspector in different entities reveal problems with compliance with the registration duties.

[113]. The main problem is the lack of awareness of entities processing data about the obligation of registration. In numerous cases these entities failed to register the data filling systems, which was only found after the General Inspector inspection. In 2006, out of 1305 decisions issued by the General Inspector 840 concerned inadequate registration[61]. Numerous mistakes occur at the registration stage, the registration form is often filled in an imprecise manner with important formal mistakes. It causes additional work for the General Inspector, which needs to inform the entities about mistakes and analyze the same form several times[62].

[114]. The General Inspector has to perform regular inspections in public administration institutions in order to verify registration (or eventual update) of the data filling system[63]. The Data Protection Law provides that every change of information concerning data processing should be notified by the authority to the General Inspector within 30 days[64]. However, in practice entities very often fail to update this information and they change it only after the General Inspector's control.

[115]. The processing of sensitive data always raises numerous doubts. The General Inspector dealt with numerous cases in that respect[65]. One of the most

60 Art. 27 par. 2 of the Act.
61 Data from the 2006 Inspector General yearly report, p. 19, report available on: http://www.giodo.gov.pl/data/filemanager_pl/1051.pdf.
62 Information provided in the 2007 Inspector General yearly report, p. 128-129, report available on: http://www.giodo.gov.pl/data/filemanager_pl/1218.pdf.
63 In 2007 Inspector General yearly report, p. 130.
64 Art. 41 par. 2 of the Act.
65 In 2007 Inspector General yearly report, p. 26-28.

significant cases concerned the director of a primary school which was collecting data of Roma children (such as the family situation, age, sex, religion and language) in order to transfer them to the Ministry of Interior (*Ministerstwo Spraw Wewnętrznych i Administracji*), which on that basis was preparing a special program for the "Roma population in Poland". The activity was based on an ordinance passed by the Minister of National Education. The General Inspector in his decision ordered the authority to delete data concerning Roma children which was processed without their knowledge and consent[66]. It referred to the fact that regulation has no supremacy over the Act, which bans the processing of such data.

[116]. Another case concerned the processing of data of election candidates by the Ministry of Interior. The Ministry was processing for statistical purposes data of election candidates from different national and ethnic minorities. The Ministry claimed that it processes only data which is publicly available (because electoral committees created by minorities submitted them). However, the General Inspector found out that the Ministry transfers also data of minorities' candidates, but who were participating in elections as members of other, non-minority electoral committees (e.g. Ukrainian origin candidate in a committee of the political party of universal membership). The General Inspector ordered the Ministry to suspend the processing of data acquired from unofficial sources, without the data subject consent[67]. The Ministry had to consent to the order of the General Inspector.

3.1. Administration of information security

[117]. The processing of data in Poland within private and public organization is effectuated by so called "ABI" – administrator of information security (administrator bezpieczeństwa danych), appointed by the entity processing data[68]. Exclusively persons who were granted an authorisation by the entity are allowed to carry out the processing of data[69]. The appointment of an ABI should be registered upon the data filing system registration. The Data Protection Law allows appointing several ABI, but only one of them should be the leader. In general, ABI should posses a special knowledge and expertise in data protection. However, the Data Protection Law does not precise any particular requirements of appointment[70].

66 Decision issued on 12 October 2007, reference: GI-DEC-DOLiS-218/07/5787, 5788.
67 Decision issued on 23 November 2007, reference: GI-DOLiS-430/103/07/6592.
68 Art. 36 par. 3 of the Act.
69 Art. 37 of the Act.
70 The organization of ABI work should be in compliance with ISO/IEC 27001, BS 7799, ISO/iEC 13335 and the Common Criteria.

[118]. In practice all employees of the entity processing data may become ABI. ABIs should posses a deep knowledge in the field of data protection, knowledge of IT and should be employed full time. Very often ABI are one of the IT officers employed by the entity, due to technical character of their work. They are performing their duties after training on data protection and are directly dependent of the entity processing data (the administrator of data).

[119]. In numerous universities special courses were created to prepare for future ABI work.

[120]. In his yearly reports the General Inspector assess the compliance and eventual lack of compliance with data protection legislation.[71] The report is based on numerous controls effectuated in fields such as public administration, public security, banks and financial institutions, health establishments, social and private insurances, archives and others.

[121]. Under the report for 2007 the lack of compliance with data protection standards in the public administration concerned particularly:

- the storage of data in inappropriate conditions, on shelves and in drawers without lockers,
- the IT systems did not meet in numerous cases the technical requirements prescribed by law,
- in isolated cases, the IT system allowed access to data filling to non-authorized persons,
- the use of data collected during administration proceedings for another goal than the purpose of administrative proceeding,
- in isolated cases, rendering public, through publication on a web site, data of persons which denied consent.

[122]. The public security sector does not reveal any particular deficiencies in the field of data protection and the institutions seam to comply with the legislation. In that field the General Inspector received numerous complaints about the processing of data by the police or the Central Anti-Corruption Office (*Centralne Biuro Antykorupcyjne*). However, in these cases the General Inspector did not find any irregularities, although those decisions were found to be controversial.

[71] Reports available on: http://www.giodo.gov.pl/156/j/pl/. The described deficiencies in data protection will be based on the more recent report of Inspector General (2007).

[123]. Banks and financial institutions revealed during the control some lack of compliance with the legislation.[72] The General Inspector particularly referred to:

- lack of appointment of ABI,
- lack of authorization of employees responsible of data processing,
- lack of evidence of persons processing data in the company,
- lack of registration of data filling systems (particularly, concerning the participants of the investment funds),
- insertion in the contracts of clauses concerning data protection misleading the signatory.

[124]. The General Inspector gave also a negative assessment of the compliance with the data protection of public health institutions. He presented such deficiencies as:

- lack of technical means of protection and processing of data,
- the storage of data in inappropriate conditions, on shelves and drawers without lockers,
- lack of control by the administrator of data entered in the system and data processed,
- no register of persons entitled to administer data processing,
- no documentation about technical and organizational measures of data processing,
- no possibility of verification of the first registration of a data subject in the system,
- lack of backup copy of data filing.

[125]. The General Inspector gave a good assessment of compliance with data protection legislation to the Nation Health Fund (*Narodowy Fundusz Zdrowia*), body responsible for financing health institutions in Poland.

[126]. The lack of compliance with data protection legislation of Public Social Security Institution (*Zakład Ubezpieczeń Społecznych*) concerned in particular the IT system of data processing:

- no file for every person of which data were processed,
- no indications about the first introduction of data subject in the system,

[72] Examples of main problems with compliance with the legislation on data protection in the banking sector are analyzed in annex 2 to this report.

- no possibility of control by whom data were introduced in the system.

[127]. Same problems with legal compliance were observed during controls of public archives.

[128]. The control effectuated in numerous other entities processing data in different commercial fields revealed the lack of compliance with:

- the obligation of information of subject data about the name, seat, address of the entity processing their data (obligation provided by art. 24 par. 1 of the Act),
- the lack of registration of data filing system (e.g. repertory of clients) with the General Inspector,
- the Labour Code provisions about the collection of data concerning employees (e.g. information about the maiden name of the employee mother),
- the entity obligation to provide with a register of persons entitled to process data,
- the technical obligations of IT systems.

[129]. In general, the General Inspector has noticed in 2007 a decrease of the number of cases where a breach of the data protection regulations occurred in comparison to previous years. Such a situation results of a large educational and information campaign conducted by the General Inspector.

.

4. Sanctions, Compensation and Legal Consequences

[130]. The Data Protection Law refers to three types of sanctions: administrative, disciplinary and criminal.

[131]. In case of any breach of the provisions on personal data protection, the General Inspector *ex officio* or upon a motion of a person concerned, by means of an administrative decision, shall order to restore the proper legal state. In particular the General Inspector may order to:

- remedy the negligence,
- complete, update, correct, disclose, or not to disclose personal data,
- apply additional measures protecting the collected personal data,
- suspend the flow of personal data to a third country,
- safeguard the data or to transfer them to other subjects,
- erase the personal data.[73]

[132]. If the General Inspector refuses to register a data filing system, he/she may order by means of an administrative decision to limit the processing of all categories or some categories of data only to the storage of data, or apply other measures presented above[74].

[133]. Decisions taken by the General Inspector are subject to administrative law regulations and may be re-reviewed by the General Inspector, and then by the Regional Administrative Court (*Wojewódzki Sąd Administracyjny*)[75] and further by the Supreme Administrative Court (*Naczelny Sąd Adminsitracyjny*).

[134]. The lack of proper financial sanctions that could be imposed by the General Inspector has been broadly criticized. An amendment of the sanction system has been proposed in December 2007 by the President of Poland. The draft amendment is actually under consideration in the Parliament.[76] The changes

[73] Art. 18 par. 1 of the Act.
[74] Art. 44 par. 2 of the Act.
[75] Art. 3 of the Act of 30 August 2002 on Proceedings before Administrative Couts, *Ustawa o postępowaniu przed sądami administracyjnymi*, Journal of Laws [*Dziennik Ustaw*] No. 153, item 1270.
[76] The draft law has been submitted to the Parliament on 21 December 2007 (official number: 488). The Sejm Committee on Justice and Human Rights has organized in July 2008 an official hearing of all stakeholders interested in amendments to the Data Protection Law.

proposed by the draft would enable the General Inspector to impose financial sanctions (from 1,000 to 100,000 euro) on the entity which fails to comply with the General Inspector decision (imposed in accordance with art. 18 par. 1 and art. 44 par. 2 of the Data Protection Law). Furthermore, the General Inspector will be able to fine the director or legal representative of an entity which obstructs proper conduct of the control. However, the draft regulation is very controversial and the final scope of the amendment may still evolve. Please note that following the submission and first reading of the draft law, there were no further works on it.

[135]. If the inspection reveals negligence of the data processing entity employee, the inspector may demand the employing entity to institute disciplinary proceedings against him. The disciplinary sanctions are provided by the Labour Code[77] and numerous regulations related to different professions. The disciplinary sanction may even lead to a termination of the employment relation.

[136]. If the inspection reveals that the action or failure in duties of the head of an organisational unit, its employee or any other natural person acting as the controller bears attributes of a criminal offence, the General Inspector shall inform a competent prosecutor, enclosing the evidence confirming suspicions[78].

[137]. The Data Protection Law provides for different types of offences related to data protection, like non-authorized data processing[79], improper data storage[80], disclosure of data to unauthorized person[81], damages, destruction of data[82], failure to notify the data filing system for registration[83] or failure to inform about the benefits, protection resulting of the Data Protection Law[84].

[138]. The general possible sanctions are a fine, a partial limitation upon personal freedom or imprisonment from one to two three years (depending of the nature of the offence). A qualified version of non-authorized data processing relates to disclosure of information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, health records, genetic code, addictions or sexual life. For disclosure of such information the offender may be sentenced up to three years of imprisonment.

[139]. Another possible remedy and way of protection is a private law lawsuit against the entity processing data. The Data Protection Law does not provide any

77 Art. 108-113 of the Labour Code of 26 June 1974, Journal of Laws of 1974, No. 24, item 141.
78 Art. 19 of the Act.
79 Art. 49 of the Act.
80 Art. 50 of the Act.
81 Art. 51 of the Act.
82 Art. 52 of the Act.
83 Art. 53 of the Act.
84 Art. 54 of the Act.

regulation concerning the civil proceedings for compensation. Therefore, the general rules of the Civil Code[85] are applicable.

[140]. The data subject may obtain *ex delicto* compensation before civil courts against the entity which infringed the processing of data rules (art. 415 of the Civil Code). In such a case the burden of proof will lay on the data subject.

[141]. The data subject may obtain compensation through the personal rights' protection system. Personal rights are e.g. name, image, and correspondence. The protection of personal rights is guaranteed in Art. 24 and 448 of the Civil Code. These articles provide that all persons whose personal rights were endangered may request a rectification of the defaming statement, just satisfaction for damages caused by the defaming statement. The just satisfaction can be awarded directly to the claimant, plaintiff or for the purpose of a social issue (e.g. Polish Red Cross). The plaintiff may also request the compensation of material damages caused by the breach of personal rights. However, the personal rights' notion is much broader than personal data and the scope of protection might vary (e.g. the Supreme Court have stated that rendering public the information on the employee salary constitutes a breach of art. 24 of the Civil Code, while it will not constitute a breach within the meaning of the Act)[86].

[142]. The Civil Code does not provide any minimum or maximum of the compensation that should be awarded. The general rules concerning the amount awarded for just satisfaction are set by the jurisprudence. The Supreme Court in its numerous judgments has set the following rules that the courts should follow while deciding on the amount of the just satisfaction:

- they should take into account the fact that the just satisfaction is a compensation and does not have a repressive character;
- they should analyze whether other, non-financial measures, would constitute a sufficient redress;
- the facts of the case, such as the reaction of the plaintiff, the rectification of the publication etc;
- the scope of the culpability of the person proclaiming defaming statements;
- the award of just satisfaction should be perceived as an ultimate mean and should be awarded only when other measures (mainly rectification of the statement) are not adequate and sufficient.

[85] Civil Code of 18 May 1964, Journal of Laws from 1964 No. 64, item 93.
[86] Please refer to case III described in Annex 2.

[143]. The General Inspector has also supervision duties and may identify data protection problems through complaints (the most common way) or through *ex officio* investigations. The inspection is usually performed by inspectors - employees of the General Inspector Office.

[144]. In order to carry out control tasks (referred to in Article 12 point 1 and 2 of the Act) the General Inspector, the Deputy General Inspector or employees of the Bureau shall be empowered, in particular to:

- enter any premises where the data filing systems are being kept and premises where data are processed outside from the data filing system, and to perform necessary examination or other inspection activities to assess the compliance of the data processing activities with the Data Protection Law,
- demand written or oral explanations, and to summon and question any person within the scope necessary to determine the facts of the case,
- consult any documents and data directly related to the subject of the inspection, and to make a copy of these documents,
- perform inspection of any devices, data carriers, and computer systems used for data processing,
- commission expertise and opinions to be prepared[87].

[145]. On the basis of the inspection findings, the inspector may demand that disciplinary proceedings or any other action provided for by law (criminal proceedings which lead to the imposition of sanctions provided in art. 49-54 of the Data Protection Law) be instituted against persons guilty of the negligence and he/she be notified, within the prescribed time, about the outcomes of such proceedings and the appropriate actions taken[88]. In case of an eventual breach of law the General Inspector has to notify the prosecutor on his suspicion and criminal proceedings would be opened against the business entity breaching Data Protection Law. In 2007, the General Inspector has notified 18 suspected offences. In 2008, this number increased to 25 cases[89].

[146]. If the inspection reveals that action or failure in duties of the head of an organisational unit, its employee or any other natural person acting as the controller bears attributes of an offence within the meaning of the Data Protection Law, the General Inspector shall inform about it a competent prosecutor, enclosing the evidence confirming suspicions[90].

---

87 Art. 14 of the Act.
88 Art. 17 par. 2 of the Act.
89 Data available on the Inspector General web page: http://www.giodo.gov.pl/246/id_art/886/j/pl/.
90 Art. 19 of the Act.

[147]. However, if the General Inspector observes some irregularities in dealing with personal data, it may issue an administrative decision by which a proper legal state should be restored. The General Inspector has no power to enforce his decisions. Accordingly, business entities quite often refuse to conform to his decisions. The General Inspector has no power to impose financial sanctions or compensation payments. To remedy this situation the General Inspector supports the amendment of the Act proposed by the President (please see above).

[148]. The enforcement of data protection legislation depends largely on the initiative of the data subject, which may lodge a complaint with the General Inspector. The General Inspector may, in turn, open administrative proceedings. However, as mentioned above, the General Inspector poses no ability to enforce his decisions through sanctions.

[149]. The General Inspector has an informative web page on which the data subject may find relevant information on the data protection legislation, on how to lodge a complaint and which are the rights deriving from the Act. The web page provides also a possibility to lodge a complaint by electronic means.

[150]. There are also numerous informal web pages providing complete information about the data protection system in Poland and the possibility to obtain compensation[91]. The General Inspector is also providing regular training within different State authorities about the data protection obligations[92].

[151]. Upon review of the complaint the General Inspector informs the data subject about the possibility to obtain compensation through civil proceedings. The General Inspector has no obligation to provide legal assistance or legal representation in compensation cases.

[152]. The legal assistance and representation in data protection cases is not institutionalised in Poland. There are no publicly founded bodies performing this function, nor established NGOs or associations performing such function. However legal aid in data protection cases may be provided within the scope of free legal aid programmes of different NGOs, such as “legal clinics” organized at almost all law faculties in the whole country, free legal aid of the Helsinki Foundation for Human Rights in certain precedent cases[93] or the Union of Citizens Advice Bureauxs (Związek Biur Porad Prawnych)[94].

[91] The web page of the Center of Data Protection, an organization providing with training on the data protection system in Poland : http://www.codo.pl/bez_kol/index1.htm.
[92] Information about education available on: http://bip.giodo.gov.pl/418/j/en/.
[93] Official web page: http://www.hfhrpol.waw.pl/.
[94] Information available on the union web page: http://www.zbpo.org.pl/page/en/.

[153]. The financial risk of proceedings in data protection cases lies generally on all participants of the proceedings. In administrative proceedings, it is the General Inspector which decides on the costs. The participant may be charged with costs that resulted from "the activity of the participant" or "from additional activity which have been undertaken by the authority on the demand of the participant"[95]. In proceedings before administrative courts participants bear costs in equal parts. However, if the court finds that an administrative decision has to be annulled or quashed, the participant may claim further reimbursement of court costs and legal representation costs[96].

[154]. In civil proceedings, financial risk of legal procedures is carried by the participant introducing a lawsuit for compensation. The general rule is that the losing party is required to cover the costs of the proceedings and the costs of legal representation[97].

[155]. In criminal proceedings the court decides who bears court fees. If the accused is found guilty, he/she may be charged with court fees and legal aid costs. However, it happens in practice rarely[98].

4.1. Protection of personal data in employment relationship

[156]. The protection of personal data in the employment relation is guaranteed by the Data Protection Law, the Labour Code and numerous specific regulations. No complex and unified regulations concerning the processing of data by employers have been introduced. When entering in the employment relation the employer may ask the name and surname of the employed person, names of the parents, date of birth, place of living, correspondence address, education and information about prior employment[99]. An employer may ask for these data already at the recruitment level.

[157]. Independently of the information mentioned above, an employer may demand from a person already employed to provide the names and dates of birth of the employee's children (if such data will enable the employee to benefit of additional privileges) and the personal electronic identification number

95 Art. 262 par. 1 of the Administrative Proceedings Code of 14 June 1960, Journal of Laws 2000, No. 98, item 1070.
96 Art. 199 and 200 Administrative Courts Proceedings Act.
97 Art. 98 par. 1-3 of the Code of Civil Procedure of 17 November 1964, Journal of Laws 1964, No. 43, item 296.
98 Art. 627 and 628 of the Criminal Procedure Code of 6 June 1997, Journal of Laws 1997, No. 89, item 555.
99 Art. 22¹ par. 1 of the Labour Code.

(PESEL). An employer may also request from the employee an evidence of the information provided.

[158]. The Labour Code does not refer to the period of time in which an employer may process data of unsuccessful candidate. This issue provokes controversies and results in different interpretational approaches. In general, an employer retains data only if a candidate gave consent for his/her data to be processed in the future (of course if the purpose of data processing will not change). In case such consent has not been given, an employer should destroy the candidates' files.

[159]. The processing of "sensitive" data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, as well as the processing of data concerning health, genetic code, addictions or sex life and data relating to convictions, decisions on penalty, fines and other decisions issued in court or administrative proceedings) by an employer is prohibited[100].

[160]. An employer, being administrator of the data, is obliged to implement technical and organisational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and in particular to protect data against their unauthorised disclosure, takeover by an unauthorised person, processing with the violation of the Data Protection Law, any change, loss, damage or destruction[101]. An employer is obliged to keep a documentation describing the way of data processing.

[161]. The Data Protection Law, however, leaves numerous aspects of data processing undetermined, left to the decision of an employer. It enables an employer to decide on goal of the data processing. It may lead to potential abuses. An employer, data administrator assesses aim of data processing and decides whether it may infringe rights and freedoms of an employee. The definition of the goal of data processing has an impact on the scope of data processing. Therefore, all data related to personnel management (e.g. psychological tests) are an enormous source of information, which in turn may lead to uncontrolled processing (e.g. causing discrimination of the data subject employee).

[162]. Trade unions have a general right to monitor compliance of an employer's actions with law[102]. It means that they also have a right to monitor employer's compliance with the Data Protection Law and other acts. Trade unions may act on their own initiative or after receiving information, informal complaint from an employee, member of the trade unions. If trade unions consider that an employer violates one of his legal obligations (including data protection) they

[100] Art. 27 of the Act.
[101] Art. 36 par. 1 of the Act.
[102] Art. 8, art. 23 par. 1 and art. 26 point 3 of the Trade Unions Act of 23 May 1991, *Ustawa o związkach zawodowych*, Journal of Laws 2001, No. 79, item 854.

may claim before the competent authority (e.g. General Inspector) launching of control proceedings[103].

[103] Art. 23 par. 2 of the Trade Unions Act.

5. Rights Awareness

[163]. We are not aware of any surveys or studies regarding data protection law and rights in the population or in special segments of society. The information on the official website of the General Inspector refers only to the survey by Eurobarometer. The current General Inspector, Michał Serzycki, when he started his term, declared his intention to intensify educational activities regarding data protection. Indeed, this effort is noticeable [see further: Good Practices]. Nevertheless, the unavoidable progress in the area of technology, in particular communication and computerization, causes many doubts on the side of data subjects and prospective data administrators.

[164]. The staff in the Office of the General Inspector confirms that most frequent issues referred to the office concern interpretation of the Data Protection Law – yearly above 1000 questions (in 2005 – 2821 questions). Apparently, most frequent questions concern definition of personal data[104] and the duty to notify a data filing system for registration. Often civil servants controlling data filing systems within public administration question lawfulness of making data processed within their statutory activity available to other public subjects. Thus, awareness of rights and duties is not always identical with certainty how to interpret the law.

[165]. There are different studies and surveys on the data protection rights awareness, conducted for different purposes and by different institutions. However, only the yearly report of the General Inspector may be perceived as a regular survey of social awareness.

[166]. The last complex report on the data protection system was realized by the Polish Centre of Public Opinion Studies (*TNS OBOP*)[105] and released on 10 .10. 2008. The report concentrated on public opinion of Poles about data protection in Poland and on the level of data protection in Polish companies[106]. The report was created on the basis of a public interviews effectuated by a telephone with more than 300 persons, randomly chosen, located all around Poland. The survey was conducted in the period from 25.09.2008 until 03.10.2008.

---

[104] For example in September 2008 the General Inspector refused intervention in a case when the full name, picture, attended school and year of graduation taken together were published on the biggest social portal against the will of the data subject justifying that such information is not identifying since identification requires an unreasonable time, cost and manpower (Art. 6 para. 1 of the Law).

[105] Official web page: http://bip.giodo.gov.pl/418/j/en/

[106] The study is available on: http://74.125.77.132/search?q=cache:xJ1aVShw0WcJ:www.giodo.gov.pl/plik/id_p/1341/t/pdf/j/pl/+raport+ochrona+danych+osobowych+w+polsce&hl=pl&ct=clnk&cd=2&gl=pl.

[167]. Private companies often conduct private surveys on topics of their interests related to data protection (e.g. in November 2008 the company Kroll Ontack[107] released a study on the awareness of companies about the protection of data stored on hard disks of useless computers).

[107] Company official web page: http://www.krollontrack.pl/odzyskiwanie-danych,1,0.html.

6. Analysis of deficiencies

[168]. Effectiveness of data protection in Poland is seriously diminished by the fact that the General Inspector lacks important competences that would strengthen its role. Although supervision by the General Inspector has helped to put the Data Protection Law into constant practice, its position between other public organs is rather weak. First, it does not have a right to legislative initiative. Second, unlike the Commissioner for Citizens' Rights, it does not have a right to take part in the proceedings before the Constitutional Tribunal either as a participant in the proceedings or as a subject making application to the Tribunal regarding abstract constitutional review[108]. Third, the system of enforcement of the Data Protection Law is flawed and leaves the General Inspector without effective tools.

[169]. Currently, the presidential draft law amending the Data Protection Law foresees a new system of administrative fines to be imposed on subjects violating the Law. Paradoxically, the General Inspector as an administrative organ could not use the system of fines foreseen in Code of Administrative Procedure since its decisions imposing non-pecuniary obligations are not enforceable in pursuance to the Law on Enforcement Procedure in Administration[109]. The Law applies to organs of local government and government administration, whereas the General Inspector is an organ of public administration supervised by Sejm (thus not a governmental organ). Once it gains the competence to issue decisions imposing pecuniary obligations, it will fall under the scope of the administrative enforcement procedure. However, pecuniary sanctions projected in the presidential draft law constitute a system parallel to this envisioned in the administrative enforcement procedure. Such solution has been strongly criticised at the session of the parliamentary commission discussing the amendment.

---

[108] Art. 191 para. 1 of the Constitution lists following subjects authorized to initiate constitutional review: 1) the President of the Republic, the Marshal of the Sejm, the Marshal of the Senate, the Prime Minister, 50 Deputies, 30 Senators, the First President of the Supreme Court, the President of the Supreme Administrative Court, the Public Prosecutor-General, the President of the Supreme Chamber of Control and the Commissioner for Citizens' Rights, 2) the National Council of the Judiciary, to the extent specified in Article 186, para. 2; 3) the constitutive organs of units of local government; 4) the national organs of trade unions as well as the national authorities of employers' organizations and occupational organizations; 5) churches and religious organizations; 6) the subjects referred to in Article 79 to the extent specified therein.

[109] Art. 2 para. 1 (1a) of the Law on Enforcement in Administration of 17 June 1966, *ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji],* unified text - Journal of Laws (*Dziennik Ustaw*) of 2002, No 101, Item 968.

[170]. The analysis of the mandate of the General Inspector naturally raises questions about limits of data protection *vis-à-vis* right of access to public information. Since the Data Protection Law foresees criminal sanctions for unlawful processing of personal data and there are practically no sanctions for failure to make public information accessible in Bulletin of Public Information [*Biuletyn Informacji Publicznej*, BIP], there is a clear tendency to deny access to public information on the account of data protection. In order to balance protection between these two areas, it is proposed to include in the mandate of the General Inspector a competence to safeguard both processing of data and access to data held by public bodies. Such change would also call for an amendment of the Law on Access to Public Information [*ustawa o dostępie do informacji publicznej*][110]

[171]. The General Inspector expressed its readiness to overtake a competence of the Minister of Interior (*Minister Spraw Wewnętrznych i Administracji*) to supervise operation and content of the websites of the Bulletin of Public Information. Such model has proved good in other countries. Currently, the Minister of Interior is in charge of operation of the main page of BIP and setting the standards and requirements for BIP.

[172]. In sum, deficiencies in personal data protection in Poland can be remedied by new or amended legislation, consequent interpretation and better application of existing laws[111]. One of the issues, which needs to be regulated in detail is outsourcing of data processing.

[173]. It should be emphasized that low numbers of public indictments in cases concerning processing of personal data do not reflect the scale of the problem. Rather, it indicates lack of understanding of the technicalities of data protection. In most of the situations when the General Inspector notified the case to public prosecutors they found low social harm of the acts and did not issue the indictment. Thus, the question is whether the criminal sanctions enshrined in the Law are not effective or they are not applied effectively.

[174]. The Association of ABIs (*Stowarzyszenie Administratorów Bezpieczeństwa Informacji*) claims that the projected expansion of the institutional system of the data protection will fail unless the internal supervisory powers of the ABIs are strengthened. Currently, their position is unclear and rather weak. It is also argued that they lack necessary independence to fulfill their functions – they should not be directly subordinated to the data controller.

---

[110] The Law of 6 September 2001, Journal of Laws 2001, No 112, Item 1198. The access to public information can be also denied on the account of protection of company secrets.

[111] It has been proposed in the parliamentary commission during public consultations on the presidential draft amending the Law that there should be a consultation board instituted at the Bureau of the General Inspector in charge of analysis of new issues raising interpretation or compliance problems.

[175]. Many problems concerning data protection can be resolved though technical adjustments in order to secure the processed data in a better way – preventing access by unauthorized persons, a theft, change, loss or damage, etc. In case of processing data in the computer systems, they require professional, regularly actualized programs securing the system from unauthorized access or interception, as well as instruction how to comply with conditions set by the Data Protection Law. Controls and inspection carried out by the General Inspector show also a need for organizational improvement of data protection by different subjects

7. Good practices

[176]. As one of good practices of the General Inspector is its educational activity. In order to perform this task the General Inspector cooperates with public institutions and private firms. The latter carried out training of their employees or adopted codes of good practices for their branch. Among them the General Inspector lists the Association of Direct Marketing [*Stowarzyszenie Marketingu Bezpośredniego*] and the Polish Federation of Real Estate Market [*Polska Federacja Rynku Nieruchomości*]. Moreover, the Office of the General Inspector cooperated with the higher education institutions like Kozminski University (previously called the Leon Kozminski Academy of Entrepreneurship and Management), the Higher School of Finance and Administration in Gdańsk and the Higher School of Business National-Louis University in Nowym Sączu).

[177]. A new initiative constituting good practice is since 2006 e-GIODO[112], the Internet platform for communication of citizens and business entities with the General Inspector. The communication may include sending petitions and notifications of the data filing systems on-line, as well for searching in already registered systems. The easy access to the registry with specified search option is of particular use of persons residing outside Warsaw. Prior to this initiative such persons could access the registry only in person in the Bureau of the General Inspector.

[112] http://egiodo.giodo.gov.pl/index.dhtml

8. Miscellaneous

Annexes

Annex 1 – Tables and Statistics

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	10.023.000	10.410.000	9.515.000	9.946.000	10.781.000	11.500.000	12.020.000	12.391.000
Staff of data protection authority	102	100	103	112	115	115	117	117
Number of procedures (investigations, audits etc.) initiated by data protection authority at its own initiative	171	250	284	258	226	171	147	185
Number of data protection registrations	2801	1814	1342	2214	2787	5344	5113	4850

Number of data protection approval procedures	35675	12561	2407	3461	3152	3175	3820	2598
Number of complaints received by data protection authority	761	795	830	753	1024	979	712	796
Number of complaints upheld by data protection authority	228	169	139	123	134	336	357	280
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)	44113 228	52 169	61 139	74 123	82 134	52 336	15 357	18 280114

[113] The IGPPD's report on an offence related to the personal data protection.
[114] Administrative decisions issued by the IGPPD being the result of the complaints received.

Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)	13	10	12	9	35	25115	-	-
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)116								

[115] Convictions for the offences contrary to the Act on the Protection of Personal Data are the only kind of quantifiable sanctions (see the table above). No data is available for the 2006-2007 period. Neither the IGPPD nor any other non-judicial body has the authority to impose civil or penal sanctions. The IGPPD issues administrative decisions remedying the infringements.

[116] Article 49
(1) A person who processes personal data in a data filing system where such processing is prohibited or where such a person is not authorised to do so shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum two years.
(2) If the offence referred to in Article 49(1) above relates to data disclosing racial or ethnic origin, political views, religious or philosophical outlook, denomination, membership in a political party or labour union, health condition data, genetic code or data regarding addictions or sexual life, the perpetrator of the offence shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum three years.
Article 50: A person who, being an administrator of a data filing system, records in the system personal data in the manner contrary to the intended purpose for which the system has been created, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum one year.

Annex 2 – Case Law

CASE I.

Case title	LG Electronics Mława.
Decision date	27 November 2008
Reference details (reference number; type and title of court/body; in original language and English	Reference: sygn. II SA/ Wa 903/08, Wojewódzki Sąd Administracyjny w Warszawie, Regional Administrative Court in Warsaw. Judgment available on web page:

Article 51
(1) A person who, being an administrator of a data filing system or obliged to protect personal data, discloses the same or enables any unauthorised persons' access thereto shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of up to two years.
(2) If a perpetrator of the above offence acts without fault, they shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum one year.
Article 52: A person who, being an administrator of data, breaches, even without their fault, the duty to protect the same from taking away by an unauthorised person, damage or destruction shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum one year.
Article 53: A person who, despite being obliged to do so, fails to register a data filing system shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum one year.
Article 54: A person who, being an administrator of a data filing system, fails to discharge the duty to inform the subject of the data of their rights and/or the duty to give such a person the information allowing them to exercise their rights granted by this Act shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of maximum one year.

[official translation, if available])	http://orzeczenia.nsa.gov.pl/cbo/do/doc?d=3062187CA08D9EFB6303A92948D6679973D35461&sc=
Key facts of the case (max. 500 chars)	LG Electronics, with its seat in Mława was taking finger prints of its employees, after they gave consent to process these data. The Inspector General in his decision stated after a control in LG Electronics, that the use of epidermal ridges in order to control the employees' working time, beginning and end of work, has been unlawful. The Inspector General stated that the company may process only data defined in art. 22^1 par.1 and 2 of the Labour Code (the name and surname of the employed person, names of the parents, date of birth, place of living, correspondence address, education and information about prior employment). The Labour Code does not refer to biometric data, including finger prints.
Main reasoning/argumentation (max. 500 chars)	LG Electronics lodged an appeal against the Inspector General decision. The company in the appeal referred to art. 23 of the Act on the Protection of Personal Data ("the Act"), which enables the processing of all sorts of data after the data subject consent. The company also highlighted that the employees were not forced to give consent as there were two systems of control of entrances and exits of employees – electronic and traditional (for employees which denied consent for the use of their epidermal ridges). The Inspector General referred to the supremacy of the provisions of the Labour Code on the Act.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Regional Administrative Court followed the argumentation of LG Electronics and quashed the Inspector General decisions. The Court referred to art. 18 of the Act which stipulates that the Inspector General may take decisions when the case concerns personal data and when there is no legal basis for processing data. The Court further stated that art. 23 of the Act gives legal basis for the processing of data - the processing of data is permitted

	only if the data subject has given his/her consent. So if the employees of LG Electronics gave consent their data can be processed by the company, as long as the authenticity of the consent is not disputed under the civil law.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court judgment is a precedence. The Inspector General gave similar decisions in numerous cases, however only in the LG Electronics in Mława case the Inspector General decision has been appealed and than quashed by the Administrative Court. The court judgment enables to companies to use biometric data (in this case epidermal ridges of employees) in order to control employees' presence at work. The judgment is perceived as being innovative and following the aim of the technological progress. The judgement was broadly commented by the media. The decision is not final; it might be appealed to the Supreme Administrative Court.
Proposal of key words for data base	Finger prints, epidermal ridges, biometric data, consent, technological progress.

CASE II.

Case title	Protection of data of clients of insurance companies (ING Nationale Nederlanden case)
Decision date	20 December 2007

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Reference: sygn. II SA/wa 1818/07, Wojewódzki Sąd Administracyjny w Warszawie, Regional Administrative Court in Warsaw. The judgment is not final a cassation appeal has been lodged with the Supreme Administrative Court in April 2008. Judgment available on web page: http://orzeczenia.nsa.gov.pl/cbo/do/doc?d=53F6D0E6FD1DEBD55BBAC896C56AD6B9DB278D8A&sc=
Key facts of the case (max. 500 chars)	During the recruitment proceedings the insurance company Nationale Nederlanden was making psychological tests to the candidates. The Inspector General received numerous complaints about unauthorized telephone offers made by Nationale Nederlanden to persons, which never transmitted their data to the company and never gave their consent for data processing. The company was acquiring information about potential clients from contractors (data about their friends, families). In June 2007 the Inspector General realised an inspection of the company, after Jacek K. lodge a complaint with the Inspector General. On 25 May 2008 the Inspector General discontinued the proceedings. After Jacek K. appeal on 30 August 2008 the Inspector General upheld his decision to discontinue the proceedings. Jacek K. lodged an appeal to the Regional Administrative Court in Warsaw.
Main reasoning/argumentation (max. 500 chars)	Nationale Nederlanden was claiming that the employee of the company received personal data of Jacek K. through his friend and that the data of Jacek K. were destroyed just after he informed the company that he is not interested by the company offer. Therefore, the company has not breached the law. In the appeal lodged by Jacek K. before the Regional Administrative Court he referred to the control proceedings of the Inspector General which have been conducted with breach of the administrative proceedings. Jacek K. mentioned that the Inspector General failed to establish the identity of the employee of Nationale Nederlanden which used his personal data. He also referred to the possibility of transmitting by the company contractors insurance offers to potential clients (members of family, friends). These persons on a voluntary basis will be able to contact the company if interested in the offer. This would prevent from illegal data processing. The Helsinki Foundation for Human Rights introduced a third party

	intervention in the case. The organization stated that the processing of data was effectuated without the consent of the data subject and was not necessary for the performance of tasks provided by law – the goal was only direct marketing of the company.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case concerned two issues: 1. the legality of processing data in the scope of marketing activity, 2. the legality of processing data from the recruitment procedure (psychometric tests). The Regional Administrative Court considered that the Inspector General decision was taken with breach of the administrative procedure, the Inspector General failed to analyse the integrity of the evidence. The Court ordered to Nationale Nederlanden to remedy to the illegal processing of personal data for the purpose of direct marketing. The Court explained that psychometric tests should be considered as "sensitive data". The processing of such data is banned.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Regional Administrative Court in Warsaw quashed the Inspector General decision. The case has an important impact on the interpretation of art. 22^1 of the Labour Code. It explains particularly which data might be transmitted to the employer during the recruitment procedure and how these data might be further processed. The Regional Administrative Court stated that the processing of data acquired by the company during the recruitment proceedings is prohibited. Data acquired during psychometric tests should be considered as "sensitive" data.
Proposal of key words for data base	Psychometric tests, recruitment, processing data for marketing purpose.

CASE III.

Case title	Biura Informacji Kredytowej (BIK) – Office for Credit Information - Access to information
Decision date	15 February 2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Reference: sygn. I CSK 358/07, Sąd Najwyższy, Supreme Court judgement.
Key facts of the case (max. 500 chars)	Anna M. took a loan in GE bank Capital Credit, soon after she cancelled the loan and paid back the entire money to the bank. A year after she tried to take a new loan in couple of other banks. She was always denied. One of the banks employees informed her that the denial is due to information received from the Office for Credit Information (BIK) which informed the banks that she is an unreliable client. BIK is an institution created by banks, which goal is to collect information about unreliable debtors and warn banks before they decide whether to approve a loan motion. Anna M. asked BIK about the data related to her. BIK stated in reply that there was no data about her and about eventual delays related to the return of her loan. BIK transmitted to Anna M. a list of banks which addressed queries about her. Despite this fact she still could not receive a loan. She lodged a complaint to the Inspector General. The Inspector General after control proceedings established that BIK was informing the data subject only about pending loans, whereas was informing banks about both, returned and pending loans. In his decision the Inspector General obliged BIK to transmit to data subjects the same information as it transmits to banks (about pending and returned loans).
Main	Anna M. lodged a civil complaint to the civil court, under the personal goods protection system (under art. 24 of the Civil Code). She claimed 30,000 PLN (approx. 8,000 euro). The first instance court dismissed the complaint stating that BIK violated her personal goods. The court explained that BIK acted in accordance with the law. BIK was

reasoning/argumentation (max. 500 chars)	transferring data received from GE bank. According to the agreement between BIK and the bank it was obliged to transfer to other banks data about the client received from the initial bank (which gave credit to the data subject, in this case GE bank capital credit). Anna M. lodged an appeal. The second instance court dismissed her appeal. Stating that the fact that BIK breached the Act on the Protection of Personal Data was not a sufficient basis to adjudicate compensation. Anna M. lodged a cassation appeal to the Supreme Court.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Supreme Court quashed the first and second instance courts judgments and remitted the case for further analysis. The Supreme Court referred to the fact that BIK breached not only the Act on the Protection of Personal Data but also the provisions of art. 51 par. 3 and 4 of the Polish Constitution, according to which "everyone shall have a right of access to official documents and data collections concerning himself" and "everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute".
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Supreme Court in its judgment underlined that BIK behaviour violated the Polish Constitution and the Act on the Protection of Personal data. The personal data protection is related to the personal goods protection system. BIK violated provisions on data protection and the right to acquire true information about personal data. BIK violated personal goods of Anna M., such as her dignity and security. This judgment confirmed the possibility of receiving civil compensation for improper data processing, through the personal goods protection system.
Proposal of key words for data base	Access to data, banks processing data, BIK.

CASE IV.

Case title	Data protection in case of transfer of a claim (debt).
Decision date	6 June 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Reference: sygn. I OPS 2/05, Naczelny Sąd Administracyjny, Supreme Administrative Court. Judgment available on web page: http://www.giodo.gov.pl/data/filemanager_pl/736.pdf.
Key facts of the case (max. 500 chars)	A.B. concluded an agreement with S.A. concerning telecommunication services. On 24 June 2002 S.A. concluded a transfer agreement (transferred A.B. debt) with an LLC company based in Piła. S.A. also transferred A.B. claim personal data. The Inspector General gave a decision in which he stated that A.B. gave his consent only to the processing of his data within the scope of the agreement with S.A. and in order to enable the realization of the agreement. The Inspector General argued that the transfer of data to the LLC company was outside the scope of the initial agreement concluded with A.B. and should be preceded by his consent. Therefore, the transfer of personal

	data violated art. 23 par. 1 of the Act on the Protection of Personal Data ("the Act"). S.A. lodged a complaint to the Regional Administrative Court (*Wojewódzki Sąd Administracyjny*) in Warsaw. S.A. claimed the possibility to transfer A.B. data on the basis of art. 509 of the Civil Code which regulates the transfer of claims. According to this provision the transfer of claim may be realised without the consent of the person concerned.
Main reasoning/argumentation (max. 500 chars)	The Regional Administrative Court stated that S.A. violated art. 23 par. 1 of the Act. The transfer of claim regulated by art. 509 of the Civil Code do not refer to personal data. The court argumentation relied on consumer protection rules - services providers may not transfer a claim without the consumer consent if the transfer affects the consumer position. Therefore, S.A. had no right to transfer A.B. claim without his consent. The Court explained that if the transfer of the claim was illegal because of A.B. lack of consent, the transfer of personal data was forbidden. S.A. lodged a cassation appeal to the Supreme Administrative Court. S.A. referred to art. 7 c of the Directive 95/46/EC of 24 October 1995, 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 (Directive on data protection). S.A. claimed that this provision enables the processing of data when it is necessary for compliance with a legal obligation to which the controller is subjected. Therefore, if S.A. had the possibility to transfer the claim it also had the possibility to process data. The processing of data was necessary for the realisation of the transfer.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The supreme Court quashed the Inspector General decision and the Regional Court judgment. The Supreme Court referred to art. 7 f of the Directive on data protection, which enables the processing of data when it is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". The Supreme Court also referred to the judgment of 14 September 2000 (The Queen v. United Kingdom Ministry of Agriculture) in which the European Court of Justice interpreted art. 7 f of the directive on data protection, stating that the goal of the directive on data protection is the protection of privacy, which should be assessed in accordance to art. 8 of the European Convention of Human Rights. The Supreme Court highlighted that the ECJ enabled processing of personal data without the data subject consent, if the processing was prescribed by law, if the processing enabled the realization of a right prescribed by law and the data were processed only to achieve the necessary goal. In order to assure a balance between interests of both parties the Supreme Administrative

	Court introduced the obligation to assess in every case the interest of parties - the one of the company and the one of the data subject (debtor). Furthermore, according to the Supreme Court the realization of the right to transfer a claim (debt) is strictly linked with the processing of data about the debtor. The consent of the data subject is not required when the processing enters in the scope of the legitimate goal, such as the transfer a claim.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The judgment unified the jurisprudence concerning data processing in case of transfer of a claim. Before this judgment was given, regional administrative courts were presenting different solutions and different legal interpretations. The Supreme Administrative Court in its previous judgments was denying the possibility of data processing due to a debt transfer without the data subject consent. However, such an interpretation could lead to abuses from the part of the debtor, which could deny giving consent for data processing in order to impede the transfer of the claim. This judgment ended a long lasting discussion on the protection of data related to debt transfer.
Proposal of key words for data base	Transfer of a claim, transfer of a debt, debtor's data, and consent.

CASE V.

Case title	Data retention by banks.
Decision date	14 September 2005

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Reference: sygn. I OSK 39/05, Naczelny Sąd Administracyjny, Supreme Adminsitrative Court.
Key facts of the case (max. 500 chars)	Andrzej U. took a loan in Bank Przemysłowo-Handlowy in Katowice in 1997. He returned the loan in 2003 and closed his bank account. However, data about his loan were still kept by the Office for Credit Information (BIK) and transferred to banks in case of a query. BIK is an institution created by banks, which goal is to collect information about unreliable debtors and warn banks about the unreliable debtor before they decide whether to approve a loan motion. He lodged a complaint with the Inspector General, claiming that his data were processed unlawfully, without his consent. The Inspector General ordered to BIK the data of Andrzej U. processed by the bank to be erased, because his loan was returned in 2003. He did not give consent for a further processing of data. The bank appealed against the Inspector General decision. In its appeal the Bank referred to the provision of its statute, which enabled the processing of data even seven years after the client closed his account or returned the loan.
Main reasoning/argumentation (max. 500 chars)	The Regional Administrative Court in Warsaw (*Wojewódzki Sąd Administracyjny*) dismissed the appeal. The court referred to art. 105 of the Banking Law (Ustawa Prawo bankowe of 29 June 1997, Journal of Laws from 2002, No. 72, item 665), which enables to banks the creation of BIK and is the basis for its activity. The court highlighted that the internal statute of a bank does not have supremacy over the Act on data processing, according to which data processing requires the consent of the data subject. The bank lodged a cassation appeal to the Supreme Court. In the appeal the bank stated that the Regional Court wrongly interpreted the Banking Law. Art. 105 of the Banking Law was the legal basis of BIK activity. According to art. 105 par. 4 of the Banking Law BIK may process data in order to provide banks with information necessary to asses the client solvency and reliability. The lack of the possibility of processing data by BIK would hinder its activity. The bank referred to art. 23 par. 1 point 2 of the Act on protection of data which allows the processing of data when "processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision".

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Supreme Administrative Court referring to art. 105 of the Banking Law stated that banks may not create an institution which will manage the scope of her own activity. If BIK had no possibility to process data (without the data subject consent) the argumentation concerning the period in which the data may be processed was pointless. The Supreme Administrative Court also mentioned the Banking Law amendments introduced on 16 June 2005. The amendments were concordant with the Regional and Supreme Administrative Court reasoning. The amendments denied to BIK the possibility to process data without the data subject consent after the loan was returned and the contract terminated. The amendments enabled to process data after the termination of the contract only if the data subject had more than 60 days of delay in paying his loan. BIK may process data up to five years after the return of the loan or the termination of the contract.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The judgment regulates the scope of BIK activity, which generated numerous complaints lodged with the Inspector General and administrative courts. The judgment referred to the sensitive issue of debtors' data retention and processing.
Proposal of key words for data base	Period, debtors' data processing, banks, credit information, banking law.