DROIT POLONAIS CONTEMPORAIN
POLISH CONTEMPORARY LAW
1999 № 1-4 (121-124)
PL ISSN 0070-7325

POLISH LEGAL REGULATIONS CONCERNING THE PROTECTION OF PERSONAL DATA IN THE LIGHT OF THE LAW OF 29 AUGUST 1997

Bogusław Banaszak*
Krzysztof Wygoda**

The long-awaited Law on the Protection of Personal Data was adopted on 29 August 1997.[1] Why was it necessary for us to wait so long for such an important act? The reasons were undoubtedly numerous, yet the major reasons for such behaviour on the part of our legislator are to be found in the pre-1989 period. Beyond any doubt, in the People's Republic of Poland, the protection of personal data played a minor role in comparison to other developed countries (such as the present-day EU Member States). The following factors contributed to that state of affairs:

1) That what was feared most in the People's Republic of Poland was the abuse of data pertaining to individuals by State organs, especially the militia, the Security Service and special military services. Therefore, public opinion regarded the protection of personal data as part of a wider problem of the protection of the individual against the actions of an undemocratic State and its organs. The question was to render impossible the manipulation and unlawful use or management of personal data as well as to create protection against their illegal collection and storage.

2) The manner of collecting and storing personal data was traditional (and usually involved manually kept record files, registers, books, etc.). This resulted in underestimating the proper administration of the collected information. Moreover, different State institutions gathered information for their particular purposes and the danger of such institutions exchanging information obtained from citizens was not recognised. Only in mid- and late 1980s did computers become more popular and computer science was applied for the collection and processing of personal data. In the first stage of computerisation, technical innovations were perceived mainly in the context of civilisational progress, and many neglected the connected dangers.[* 1 2]

* Professor of Constitutional Law, University of Wroclaw.
** Assistant at Constitutional Law Institute, University of Wroclaw.

[1] It was published on 29 October 1997 in *Dziennik Ustaw* [Journal of Law] no. 133, item 883.

[2] This phenomenon had a broader scope. Not until 1990 did the General Assembly of the U.N. adopt Guidelines on the administration of computerised personal data. For more on this issue, see S. R e d o: "Policja a prawa człowieka w systemie Organizacji Narodów Zjednoczonych" [Police and Human Rights in the United Nations Organisation System] [in:] A. R z e p l i ń s k i (ed.): *Prawa człowieka a policja* [Human Rights and the Police],

3) Before 1989, the main interest of the citizens was to create conditions for the development of freedom of expression. Obviously, in this situation, the imposing of restrictions on making information public or obtaining it was of secondary importance. This applied also to personal data.

The issue gained more importance in the 1990s, mainly due to far-reaching political, social and economic transformations initiated after the conclusion of the Round Table Agreements. Another reason for taking greater interest in matters concerning the protection of personal data was that more and more State institutions, private enterprises and companies, etc. were beginning to use computerised information systems.

A scientific discussion (although not a very heated one) followed. In its course, emphasis was placed on the necessity of adopting Polish legislation in this field to the standards introduced by international law and to the requirements of a democratic state of law.

The discussion disclosed, apart from rather general opinions, also those which focused on certain aspects of personal data protection and on specific needs connected with solving practical problems. The main focus here was the so-called "lustracja", in whose context archives of the Ministry of Internal Affairs were usually perceived as incomplete. It was stressed just as often that in practice this state of affairs renders impossible the providing of accurate information about persons co-operating with the former special services of the People's Republic of Poland, at the same time trying to prove that in such conditions available data could not be examined thoroughly and objectively.[3]

The following needs were raised:

- to ensure the fulfilling by organs of State administration of the obligation to provide courts and citizens with information important for the latter, such organs having access to this information;
- to reduce the scope of information to be requested from citizens by State organs and to limit it to data necessary for the purpose for which it is collected;
- to create mechanisms for achieving professionalism in handling personal data in the possession of both State institutions and private companies or enterprises (with particular focus on the need to introduce restrictions as to the transference of data between such subjects and to prevent unauthorised persons from enjoying access to the compiled information);

Legionowo 1994, p. 205. However, in Europe, the dangers associated with automatic data processing were noticed much earlier, as can be seen from the activity of organs of the European Council, which dealt with this problem already in the early 1970s; it suffices to quote two acts: Resolution 22(73) of the Convent of Ministers of the EC, adopted on 26 November 1973, "Protection of natural persons' privacy with regard to electronic data banks in the private sector" (text in: *Collection des recommandations, resolutions et declarations du Comité des Ministères portant sur les droits de l'homme 1949-1987*, Strasbourg 1989, p. 89 and following) and Resolution 29(74) of the Convent of Ministers of the EC, adopted on 20 November 1974, "Protection of natural persons' privacy with regard to electronic data banks in the private sector" (text in *Collection...*, p. 44 and following).

[3] See, among other sources, B. B a n a s z a k: "Lustracja i dekomunizacja w Polsce w świetle praw jednostki w prawie wewnętrznym i międzynarodowym" [Lustration and Decommunization in Poland in the Light of Rights of the Individual in National and International Law] [in:] B. B a n a s z a k (ed.): *Prawa człowieka. Geneza, koncepcje, ochrona* [Human Rights. Genesis, Conceptions, Protection], Wroclaw 1993, and references therein.

- to promote adequate understanding and awareness of the problems of data protection among both civil servants and other subjects gathering such data;
- to hold a public discussion on the protection of personal data and the right to privacy.

Considering that until 1997 there was no comprehensive statutory regulation covering the protection of personal data in its broadly understood processing, we will refrain from an analysis of legal instruments which regulated partially the matters discussed here.[4]

We cannot, however, fail to mention the Law on Accounting of 29 September 1994[5] and Chapter 8 thereof entitled "Protection of Data". This was the first time that Polish legislation contained such a relatively broad regulation of certain aspects of the issue of interest to us. Article 71 of this law states that the documentation of adopted accounting rules, account books, stocktaking records and financial statements shall be stored in due manner and protected against illegal modifications, unauthorised disclosure, damage or destruction.

This law, again for the first time in Polish legal order, defined unequivocally the notion of the protection of data. According to Article 71, para. 2 thereof, if accounting books are kept in a computerised manner, the "protection of data shall consist in using damage-proof data carriers, properly selected external security measures, systematic creation of back-up files for data saved on magnetic carriers, as well as ensuring protection against unauthorised access to computer software".

The above mentioned law regulates also the place and manner of storing accounting books, stocktaking records and accounting evidence, specifies the minimum period of storage thereof (Articles 72 to 74) and determines the principles for making data files or parts thereof available to third persons (Article 75).

Before the Law of 29 August 1997 on the Protection of Personal Data was adopted, it would have been difficult to find any coherent and comprehensive system of legal norms for the purpose of protecting the right of privacy, ensuring, at the same time, that the individuals concerned have access to information about themselves, which is in the hands of subjects dealing with personal data processing. The first indispensable step towards creating such a coherent whole was finishing the work on the law mentioned above. Naturally, it will be necessary to develop and complete it by means of acts of lower rank, as well as careful control of the process of its implementation and, later on, observance of the standards imposed thereby on all subjects covered by its scope. It is, however, worth examining the most important regulations of this law more closely and to attempt some conclusions.

---

[4] For instance, Article 2, para. 1, subpara. 2 of the Law of 14 December 1982 on the Protection of Official and State Secrecy, the so-called "Lustracja" Law of the Sejm of 28 May 1992 or Article 81, para. 5, subpara. 4 of the 1993 Sejm Election Ordinance. For more on this subject, see B. B a n a s z a k: "Prawo do ochrony danych osobowych w Polsce" [The Right to the Protection of Personal Data in Poland] [in:] T. J a s u d o w i c z, C. M i k [eds.]: *O prawach człowieka w podwójną rocznicę Paktów. Księga pamiątkowa w hołdzie Profesor Annie Michalskiej* [On Human Rights on a Double Anniversary of the Treaties. A Commemorative Book in Honour of Professor Anna Michalska], Toruń 1996, p. 251-254.

[5] *Dziennik Ustaw* of 1994, no. 121, item 591.

1. The law covers the whole of the matter, irrespectively of the method of processing data (electronically or manually),

a) Its scope covers both traditional collections of personal data, that is record files, books, indices etc., and those contained in computer information systems. It can be said, therefore, that the Polish legislator did not consider it necessary to regulate the protection of data separately and according to where and in what form they are stored. It should also be observed that the resolutions of the Convent of Ministers of the European Council include a number of acts calling for a special treatment of electronic data banks, due to greater potential danger connected with them. Thanks to such a comprehensive regulation, any attempts to evade the norms introduced by this law, for instance, on the part of dishonest administrators who might try to do so by changing the manner of processing data from electronic to manual, are halted. It should be also borne in mind that this statutory regulation is the result of a relatively low, as compared to European (EU) standards, computerisation of both Polish administration and economy, in spite of continuous efforts. This fact, however, does not affect the justifiability of legislators' action. Furthermore, it is right, even for reasons of legislative technique, that related matters should be regulated in one legal instrument, although embracing such a broad issue must present a major problem. This does not obstruct rendering the provisions of this law more specific by other legal instruments, for example regulations (by a Minister competent as regards administration matters), referred to in Article 45 of the Law on the Protection of Personal Data, concerning basic technical and organisational requirements to be met by devices and information systems used in processing personal data, as well as those determining samples of requests or applications and specimens of official identity cards for employees of the Bureau of the Inspector General for the Protection of Personal Data (BIGPPD), the said instruments being necessary for meeting formal conditions for the functioning of the institutions created by the legislator.

b) The law defines broadly the group of subjects obliged to observe its provisions.

- ALL persons are granted the right to the protection of personal data, as specified in Article 1, para. 1. This complies with the provisions of Articles 37 and 51 of the Constitution (which find their statutory amplification in the law in question), where the subject entitled to protection is also determined broadly (no one in Article 51, para. 1 and everyone in paras. 3 and 4 thereof) and should be understood as every natural person (see also Article 2, para. 1 of the Law on the Protection of Personal Data); only para. 2 of Article 51 makes reference to citizens, which entails that public authorities can process information concerning other persons, and moreover such data need not meet the condition of necessity in a democratic state ruled by law.

- Taking into account subjects processing personal data, this law applies to State and local government units, as well as to other State and communal units, and non-Statc subjects involved in the performance of public duties and to natural and legal persons and organisational units without legal personality, which process data as part of their economic or professional activity, or for the achievement of their statutory objective; for such subjects to be covered by this law it is sufficient that they have their seat

or place of residence in the territory of the Republic of Poland or, if they do not meet this condition, that they process data using technical means located in this territory (Article 3 of the Law on the Protection of Personal Data).

- Such a broad definition of the group of subjects covered by the provisions of this law will hopefully allow to include all subjects concerned, and the exceptions the law provides for, such as an exception to the obligation to register a data file or to make known the very fact of processing it (guaranteeing the rights and interests of the persons to whom the data pertains), are in principle obvious, and serve solely the purpose of facilitating the work of the organs involved in the implementation of the provisions of this law.

c) This law, amplifying the above mentioned Article 51 of the Constitution, regulates also **basic rights of persons to whom the data pertains and the rights and obligations of subjects resulting from the fact of processing personal data by those subjects.** First, we will examine the rights of subjects to whom personal data pertains. Undoubtedly, one of the most important among such rights is the right of access to data files exercised thanks to the possibility of control over data processing, in particular through obtaining detailed information on: the very fact of the existence of a data file, the purpose, scope and method of processing the data contained therein, its administrator, the source of data and the possibilities of making data available, as well as the right to demand supplementing, updating, or correcting personal data, a temporary or permanent suspension of their processing or deletion if they are incomplete, outdated, untrue, or have been obtained in violation of the law, or are not necessary for the achievement of the purpose for which it has been compiled: (Article 32 of the Law on the Protection of Personal Data).

The most important obligations of a data administrator mentioned by the legislator included:

- **the obligation to register a data file** (Article 40 of the Law on the Protection of Personal Data), upon which the possibility of commencing the processing data is contingent (Article 46 of the Law on the Protection of Personal Data);
- **the obligation to inform the person, whose data is being collected,** about the purpose, identified or intended recipients thereof, the right to review and verify the data, the obligation, or an absence thereof, to provide the information the administrator is interested in (and, naturally, the legal basis for this obligation), and to provide full information allowing the identification of the administrator (Article 24 of the Law on the Protection of Personal Data);
- **the obligation to properly secure data files** (Chapter 5 of the Law on the Protection of Personal Data) expressly requesting administrators to apply such technical and organisational means so as to ensure the safety of processing the data contained therein. In particular, data should be secured from being provided to unauthorised persons, from being removed by non-cntitled persons, and from damage or destruction. The logical conclusion from this obligation, included in this law *expressis verbis*, is that only the persons authorised by the administrator can be admitted to operating the information system and devices constituting its parts, involved in the processing of data.

Such persons are, of course, obliged to secrecy as regards the information they have learned, even after the termination of their employment (Article 39, para. 1 of the Law on the Protection of Personal Data). This seems to be an attempt to define (create) a new kind of professional secrecy, apart from the traditional variety; in some respects, journalists' or doctors' secrecy is accompanied by something we could call information secrecy (even although it applies to an equal extent to persons having access to data processed outside electronic systems - which results from the fact that neither Article 36 nor Article 39 of the Law on the Protection of Personal Data distinguish between obligations imposed on data file administrators with regard to the method of processing data; this term seems to convey well the nature of such secrecy, the more so because we encounter this kind of secrecy in international law concerning electronic data processing. However, we cannot exclude the possibility of another, more adequate, term being coined and accepted in Polish science). In order that the obligation to ensure this special kind of professional secrecy does not remain a void provision, the legislator envisaged (in Articles 51 and 52 of the Law on the Protection of Personal Data) sanctions for disclosing the data to unauthorised persons or providing them with access. It is worthwhile to refer to the text of the law and quote the relevant provisions, paying attention to the special treatment of the obligation to protect data on the part of administrators, as they are not only accountable irrespectively of the form of the offence (since this applies also to other persons under the obligation to protect the data), but also irrespectively of whether or not a leakage of information has actually taken place. Article 51, para. 1 provides that "Any data administrator, or a person obliged to protect personal data, who discloses it to unauthorised persons, or provides them with access to the data, shall be subject to the punishment of a fine, or partial or total limitation of personal freedom of up to two years". Para. 2: "If the offence is unintentional, the offender shall be subject to punishment of a fine, or partial or total limitation of personal freedom of up to one year". Article 52: "Should a data administrator infringe - even without any intention to do so - upon his duty to secure the data from being removed by an unauthorised person, from damage or destruction, he shall be subject to punishment of a fine, or partial or total limitation of personal freedom of up to one year. Data administrators are also under the **obligation to ensure current supervision of the possessed information,** since they are to control: what personal data was introduced into the file, when and by whom, as well as to whom it is provided, especially when it is transferred by data teletransmission devices. Naturally, those regulations meet European standards expressed in the resolutions mentioned in footnote 2: No. 22(73) and No. 29(74) of the European Council (in the first resolution, concerned with the private sector, paras. 7 to 9 of the Annex, and in the second one, covering the public sector, paras. 6 and 7 of the Annex). Since the content of Resolution No. 29(74) is, in principle, a repetition (and, in some respects, a specification) of the most important provisions of the former Resolution, No. 22(73), there is no point in quoting both those acts; therefore, we will limit ourselves to listing the most important principles contained in the above mentioned paragraphs. Those principles are: (a) applying due diligence to correct imprecise information and to remove outdated information or information obtained in an illegal way;

(b) undertaking security measures to prevent any abuse of data, and harmful or prohibited use thereof; for this reason electronic data banks should be protected by systems which make it impossible for persons who have no right to obtain such information to enjoy access, and, at the same time, would make it impossible to make known distortions of information, whether accidental or not; (c) limiting access to information to a group of persons whose lawful interest is to have knowledge about such data in order to perform their duties; (d) obliging the persons involved in operating electronic data banks to observe norms preventing the illegal use of the information, and in particular, binding them by secrecy. Of course, our national regulations meet also the standards determined in Directive 95/46/EC of the European Parliament and the Council 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*, Articles 16 and 17.[6]

d) The fact that this law can be considered as covering all the problems connected with the protection of personal data in the broad understanding of the term results also from the legislator's definition of the concept of data processing as any operation on personal data, in particular collecting, saving, storing, arranging, changing and deleting, especially if such operations are performed by means of information systems. This definition of processing goes beyond the intuitive understanding of this term, yet it seems to convey - and this fact should not escape notice - the meaning of the term ***processing of personal data,*** which is used in the legal instruments of the European Union. As an example we can cite the already mentioned Directive 95/46/EC of the European Parliament and the Council, which constitutes a crucial regulation in this field. In Article 2, containing basic definitions, sub-para, b) reads: **processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.** Generally speaking, the operations in question are: introducing, storing or combining, altering, using and communicating data, including transmission, dissemination, protection, correction and erasure. This compatibility with the Polish regulation acquires special importance if we take into consideration Poland's aspiration to join the Member States and the consequent necessity to adjust its legal system.

2. Not only does this law **formulate certain rights and obligations which should serve the purpose of providing greatest possible protection of personal data, but it also attempts to create conditions necessary for its observance.** Certain regulations of special importance as regards the right of access to information can also be found here.

[6] Text in: *Official Journal of the European Communities* of 23 November 1995, no. L 281, p. 31 and following.

Creating the institution of the Inspector General for the Protection of Personal Data is the most important guarantee from the point of view of granting an individual the right of access to data files and control of their content (the position and prerogatives of the IGPPD will be discussed later); furthermore, those solutions aim at fulfilling and specifying more general provisions (such as those of Article 23, which describes conditions of the admissibility of data processing). Among those solutions we can mention the following:

a) **The obligation to collect only data which is not superfluous for the purpose for which its collection has been undertaken,** which results from Article 35, para. 1. Such purposes must, naturally, be defined and lawful. Further processing of such data should not, in principle, be inconsistent with those purposes, and the data should be correct and adequate for the purposes (Article 26, para. 1, sub-paras. 2 and 3 of the Law on the Protection of Personal Data).

b) General prohibition of processing data concerning **a person's health, genetic code, addictions or sexual life, as well as data disclosing:**

- **racial or ethnic origin;**
- **political views;**
- **religious or philosophical beliefs;**
- **denomination, party or union membership.**

Naturally, it should be observed that there exists a number of exceptions to this prohibition conceived as a general norm; however, there are, in principle, no questions as to the purposefulness of providing for those exceptions. Their existence guarantees full protection of the mentioned data categories or makes processing contingent upon the consent of the person to whom it pertains.

The expression in "principle" has not been used because of excessive caution or to avoid responsibility, since the rather vague permission to process such data, if necessary for the "performance of the duties of data administrator in relation to the employment of persons, when the scope of processing is defined by this Law", may cause misgivings that employers would be unwilling to employ certain groups of would-be employees, for instance women during the first months of pregnancy or HIV carriers (although Articles 32 and 33 of the Constitution of the Republic of Poland guarantee equality and prohibit any discrimination). Reference to statutory law gives good reason to hope that this scope will not turn out to be too wide, and that it will exclude the possibility of abusing the knowledge of such data, in particular data concerning health in its broad understanding. Although another unquestionably justified exception (even by the fact that in this case we are no longer dealing with any kind of secrecy) concerning processing data made public by the person to whom it pertains does not seem, at the first glance, to give rise to any misgivings, we are compelled to reflect on how the conditions necessary for classifying certain behaviour as rendering data public will be defined and interpreted in practice (Article 27 of the Law on the Protection of Personal Data).[7]

[7] The list of conditions for admissibility of processing contained in Article 27 of the Law on the Protection of Personal Data is not exhaustive. Other directives, formulated in general terms, are to be found in Articles 1 and 23 of the Law on the Protection of Personal Data, and will be discussed in the conclusions from the point of view

c) There exists a category of data which can be processed only on the basis of a law providing for it. This group includes data on sentencing, adjudication on penalties, fines, and other rulings issued under judicial or administrative proceedings (Article 28, para. 1 of the Law on the Protection of Personal Data).

d) Among the guarantees of privacy, we also find one from Article 26, para. 1, sub-para. 4, requiring administrators to ensure that data is stored in a form enabling the identification of the persons concerned no longer than the moment the purpose of processing has been achieved.

e) In order to avoid the danger of discrimination and to allow individuals to control the content of information pertaining to them and possessed by the State organs, it is forbidden to include any secret meaning into the elements of ordinal numbers in registration systems for natural persons; when such numbers are used in population registration systems they may contain only the designation of a person's sex, date of birth, number of entry and control number.

f) It is significant that Article 7, para. 5 of the Law on the Protection of Personal Data contains the specification of conditions required for the consent of the person concerned. Such consent should be a declaration of will, which contains consent for processing the personal data of the person submitting such a declaration; consent may not be presumed or implied from any other declaration of will. For certain categories of data such consent must be given in a written form.

3. Let us now briefly discuss that part of the law, which deals with the organ for the protection of personal data, considering that this organ exercises considerable (even though often indirect) influence upon the individual's right to respect for his private life.

At the beginning, we should emphasise that **it was necessary to establish one centralised organ in charge of registering files, exercising control over them and performing other functions connected with the protection of personal data.**

The reason was that in Polish conditions it was impossible to vest any of the hitherto existing State organs with supervisory, informative and advisory functions. It would be acceptable to assign the registration of personal data files (which would mean managing a register of data files and providing information on registered files, according to Article 12, sub-para. 3 of the Law on the Protection of Personal Data) to one of the courts (e.g. a registration court). It would have to be, however, considered a misunderstanding if such a court were to:

- present opinions on bills relating to the protection of personal data;
- initiate and undertake steps to improve the protection of personal data;
- participate in the work of international organisations and institutions involved in the protection of personal data.[8] Those do not belong to the tasks of the judiciary; more

---

of the compatibility of this law to provisions of the ECHR. All those regulations comply also with other international norms (e.g. Recommendations of the European Council and its Convention for the protection of individuals with regard to automatic processing of personal data of 28 January 1981) and EU norms - see, for example, the already mentioned Directive 95/46/CE.

[8] See Article 12, subparas. 4 to 6 of the Law on the Protection of Personal Data.

duties of the IGPPD are specified in Article 12 of the Law, especially since the expression "in particular" means that the list is by no means exhaustive. On the other hand, if we wanted to assign the functions of the Inspector General to one of the organs of State control and law protection, such as the Supreme Chamber of Control or the Commissioner for Citizens' Rights Protection (the National Council of Radio Broadcasting and Television being absolutely out of the question), we would provoke a situation in which supervision over the consistence of data processing with regulations on personal data protection (Article 12, para. 1 of the Law on the Protection of Personal Data), the issuing of administrative decisions and consideration of complaints about the application of provisions on the protection of personal data (Article 12, para. 2 of the Law on the Protection of Personal Data) would be vested in institutions whose original designation, although overlapping the new duties, would rather hinder performing the functions of an impartial organ protecting personal data. In the case of the Supreme Chamber of Control, we would certainly observe reluctance on the part of subjects, previously not subjected to control by this institution, but which, being data administrators, would be subjected to it. One should also consider the potential danger associated with access to data files by the organs concerned, and the possibility of using information obtained in this way in other fields of their activity. Besides, both courts and the Supreme Chamber of Control or other organs, which could possibly be taken into account, already perform many other duties (some say too many), and as a result the time necessary for dealing with any matter becomes increasingly prolonged.

Summarising, if the Inspector General for the Protection of Personal Data is to enjoy public confidence (which will be necessary for this organ to be efficient), it should be impossible for the Inspector to use the obtained information for purposes other than its protection. This person must be absolutely neutral, and for this reason the provisions of the law require, among other things, that he/she have outstanding moral authority, relevant knowledge and education and no criminal record. The Inspector's autonomy results also from the fact that he/she is appointed by the Sejm, subject to approval by the Senate, and during the four-year term of office he/she is subject only to this law, being granted formal immunity equal to that of a deputy. As we know, however, gaining public approval and autonomy of actions would not constitute a sufficient basis to consider the Inspector an efficient organ, if he/she had not been granted adequate instruments of control and supervision over personal data files. **Practice will show whether the prerogatives granted to the Inspector General by this law are sufficient.** In the meantime, it is worth examining some of the provisions aiming, in the legislator's opinion, at granting such a position to the Inspector.

a) It is obvious that the IGPPD alone would not achieve anything; this is why he/she is helped in the performance of duties by the Bureau of the IGPPD and the employees of the Bureau, referred to as inspectors (Article 13 of the Law on the Protection of Personal Data). In order to perform duties connected with exercising control, issuing decisions and considering complaints, the Inspector General and authorised inspectors are granted rights typical for such cases: the right to enter the controlled quarters (between 6 a.m. and 10 p.m.) and to carry out the necessary research, the right to demand

oral or written explanations and to call and question persons, to the extent necessary for the determination of the actual state of affairs, or the right to demand the presentation of documents and any information directly related to the inspection.

b) On the basis of the findings of the inspection, the Inspector may demand that disciplinary proceedings (or other proceedings prescribed by law) be instituted against persons responsible for the violation of the regulations on the protection of personal data.

c) However, the most important supervisory right of the Inspector General, where a violation of the regulations on the protection of personal data has been found to have taken place, is the possibility to order a data administrator, by way of administrative decision *ex officio* or upon a motion of the person concerned, to restore the proper legal state. This may be achieved in particular through: (a) removing any transgressions; (b) completing, updating, correcting, making available, or not, personal data; (c) introducing additional means of safeguarding the data; (d) withholding any transfer of personal data outside the Polish borders; (e) securing the data or transferring it to other subjects; (f) deleting personal data.

d) In those cases when a violation of the penal provisions of this law has been found, the Inspector General is also under the obligation to inform a proper investigative body of the commission of the crime.

This law, however, allows considerable autonomy for data administrators, as can be seen with regard to administrators of data files compiled solely for technical or educational reasons, or in relation to teaching in schools of higher education, when the data is deleted or made unidentifiable immediately after use, since they are only required to observe the provisions of Chapter 5 concerning the safety of files (Article 2 of the Law on the Protection of Personal Data). The exclusions from the duty to register data files, applicable to administrators of data specified in Article 43, have a similar meaning, because as regards such data the Inspector General does not enjoy control and supervisory powers. Nonetheless, the categories of specified data are varied, starting with **data files concerning vital interests of the State and the judiciary and covered by State secrecy due to State defence or security, protection of the life and health of people, protection of property, and public safety and order,** those processed by appropriate organs for court proceedings or those concerning persons deprived of personal freedom on the basis of statutory law, to the extent necessary for applying temporary arrest, or for punishment in the form of imprisonment. We find also data files **administered by subjects closely linked with the persons whose data is being processed,** such as those concerning persons employed by them, associated with them, studying at their facilities, receiving medical services, notary, attorney or legal counsel services, or those processed exclusively for the purpose of preparing invoices, bills or financial reports. Finally, we come across **data files which are generally available or are processed for minor everyday matters.**

This law does not deprive administrators of the possibility to transfer data abroad as long as the recipient country guarantees protection to an extent corresponding at least to Polish standards; even if it does not, after certain conditions are fulfilled (e.g.

the person to whom it pertains gives a written consent or the data is generally available), the information can be transferred (Chapter 9 of the Law on the Protection of Personal Data).

It is worth observing that on several occasions the legislator provides for not obstructing scientific research, for instance, by exempting data files, processed for a scientific dissertation required for a diploma in a school of higher education or a scientific degree, from the duty of registration. Besides, if data had been collected from persons other than those to whom the data pertains, the administrators are not required to inform the persons concerned of this fact as long as the data is necessary for scientific, didactic, historical or statistical research, or for public opinion polls and, naturally, as long as its processing does not violate the rights or freedoms of the persons concerned, and informing them would incur excessive costs or jeopardise the achievement of the objective of the research.

Data administrators have the right to appeal against any decisions of the IGPPD, usually by way of an application for a review of the given case.

Let us finish our brief discussion of the provisions of this law, and go on to summarise and evaluate its content.

The first conclusion to be drawn is that all regulations of this law manifest the legislator's desire to make all effort in order to ensure the compatibility of Polish norms with international standards, especially regional European and EU standards. The law in question respects the European Convention of Human Rights (although the latter does not mention explicitly the right to the protection of personal data, it does guarantee the right to respect for private life, from which such protection is inferred) both the guarantees of human rights and clauses introducing the possibility of limiting them (Articles 8 to 11 of the ECHR). The Polish Law on the Protection of Personal Data states in general terms that "Processing of personal data may be performed for public benefit, the benefit of the person to whom the data pertains, or for the benefit of third persons, within the scope and procedure specified by this Law. (Article 1, para. 2) and that "The data may only be processed if: 1) the person to whom the data pertains has given his/her consent, except when the data is to be deleted; 2) legal regulations allow it; 3) the person concerned needs it in order to fulfil an agreement to which he/she is a party, or, at his/her request, to take the necessary steps before entering an agreement; 4) it is necessary for fulfilling the tasks defined by law for public benefit; 5) it is necessary for achieving data administrators justified goals (...) and the processing itself does not violate the rights and freedoms of the person concerned. 2. The consent referred to in para. 1, sub-para. 1 may also be applied to future processing of the data if the purpose of the processing remains unchanged. 3. Should processing of the data be necessary for the protection of vital interests of the person concerned, and fulfilment of the condition described in para. 1, sub-para. 1 be impossible, the data may be processed without the person's consent until such a consent is obtained" (Article 23).

The law complies also with the already mentioned recommendations and guidelines of the European Council and of the Convention (EC) *for the protection of individuals with regard to automatic processing of personal data* of 28 January 1981, to whose

ratification there will be no obstacles for the legal state after the entry into force of this law, even if the adopted degree of protection comprises only minimum and extended standards, and with the extended scope of its application covered by the application of the Convention of such personal data files, which are not processed automatically (so far, our country has not done so). Let us remember that the aim of this Convention (as stated in Article 1) is to ensure that in the territories of the Member States everybody, irrespective of citizenship and place of residence, enjoys the protection of his fundamental rights and freedoms, and in particular, the right to respect for his personal life with regard to the automatic processing of personal data. Further on, the Convention deals with specifying admissible methods of obtaining and gathering personal data, which should be adequate and of appropriate quality. It provides also for introducing security guarantees and specified procedures for exchanging data, transferring it and access to it by persons to whom the data pertains.[9] The Polish law corresponds also with the above mentioned Directive 95/46/EC, whose provisions are often reflected in our document.

Secondly, the legislator has, in principle, managed to fulfil the postulate of the coexistence within one legal instrument of legal norms ensuring the protection of personal data and those concerning the conditions of access to data files, especially as regards official information.[10] It seems, however, that the Polish system of the protection of personal data places the preservation of the confidentiality of such data and the protection of private life over the right of access to information (but within reasonable limits). One of the reasons for such a state of affairs may be the fact that finding balance between those two values is sometimes extremely difficult, and information, once disclosed, cannot be made secret again.

Thirdly, one may harbour justified hope that after a full implementation of all the provisions of this law, certain negative phenomena should disappear from our life, considering that they result from an underestimation of the protection of personal data. Such phenomena include the excessive diligence of data administrators, disclosed in

---

[9] Articles 5 and 6 of this document state, among other, that the data shall be: (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible to those purposes; (c) adequate, relevant and not excessive in relation to the purpose for which they are stored; (d) accurate and, where necessary, kept up to date; (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which they are stored. Moreover, Article 8 of the Convention obliges its signatories to ensure that everybody has access to the data relating to him. Any derogations from the provisions of the Convention shall be provided for by national legislation of Member States and constitute a necessary measure in a democratic society in the interests of State security, public safety, the monetary interests of the State or the suppression of criminal offences, as well as in protecting the data subject or the rights and freedoms of others. As we can see (especially in the conditions for introducing restrictions) this document fully respects the provisions of the ECHR, and, taking into account Poland's openness to international standards of the protection of human rights, it is worth including it in the set of conventions safeguarding their observance, ratified by our country.

[10] One example of such a postulate might be the Recommendation of the Parliamentary Assembly of the EC 1037(1986) *protection of data and freedom of information,* which expresses the fear that separation of legal regulations and actual management of data protection and access to information may lead to collisions, and for this reason it is advisable to correlate those two issues, since they are part of the overall information policy within society.

including in the records information irrelevant for a given cause, or the use of old slips and forms, practised in many offices, requiring citizens to provide information unnecessary for the purpose of filling them (caused rather by a shortage of resources than by bad will). We should, however, observe that if shortly after this law's entry into force[11] its provisions are to be observed too strictly, this situation can give rise to many conflicts leading to unnecessary social tension. The standards imposed by this law will require numerous adaptive amendments in our legislation, but also (and possibly, above all) in the mentality of the subjects to whom it is addressed.

Unfortunately, we note that the application of the law in question is practically impossible in the cases of abuse connected with processing personal data in international information networks, such as the Internet. It is quite possible and feasible for subjects other than domestic ones to create personal data banks (relating to Polish citizens as well) outside the territory of Poland and without using technical means located within Polish territory as a result of the fact that this law is inapplicable (of course, we do not suggest covering such data files by the provisions of the law, as this would not be practicable). Assuming that such data could be collected contrary to Polish statutory law, for example, stolen or made available by unauthorised subjects, we must consider as very negative the fact that the law in question lacks a general prohibition against domestic subjects (both natural and any other persons) using (processing) personal data obtained from illegal sources (the liability being borne by persons responsible for the leakage - if they are identified). It may happen that at a generally accessible (network) address we will find all the information concerning not only well-known persons, but even ordinary people. This situation, confronted with the lack of an obligation to check the origin of the data (even formally: whether the file has been registered in Poland, unless we assume that the duty of an administrator,[12] resulting from Article 26 of the Law on the Protection of Personal Data, to do his/her utmost to protect the interests of the persons concerned, and, in particular, to ensure that the data is processed legally, requires him/her to check the legality of the source) precludes the possibility of applying Article 49 of the Law on the Protection of Personal Data, which prohibits processing personal data wherever such processing is inadmissible or when a given subject has no title to do so, since in such situations the requirement expressed in Article 25, para. 2, sub-para. 2 of the Law on the Protection of Personal Data is met (the data to be collected is generally available); if the purpose of processing is lawful, such a subject will undoubtedly be entitled (if he/she records the existence of the file), and will enable the administrators of files (in this case, even domestic ones) not to inform data subjects of the very fact that their files contain information pertaining to them.[13]

---

[11] This law came into force in its entirety in May 1998.

[12] Only a data administrator, and not every user.

[13] In order to illustrate, this problem, we will use two examples. 1. A personal data administrator is, in principle, obliged to register his/her data file (Article 40 of the Law on the Protection of Personal Data). Then the IGPPD (pursuant to Article 23, para. 1, subpara. 5 and Article 44 thereof) can, by way of administrative decision, refuse to register a file with regard to a violation of the rights and freedoms of the persons concerned (despite the administrator's vital interest in processing the data pertaining to such persons). Therefore, referring to Article 44

One more final remark, this time from the point of view of constitutional law. It is regretful that the IGPPD has not been included into our new Constitution. He could have been mentioned in Chapter IX together with such institutions as the Supreme Chamber of Control, the Commissioner for Citizens' Rights and the National Council of Radio Broadcasting and Television, or in Chapter II, similarly to the Commissioner for Children's Rights. Since this chapter contains Article 51, which is crucial for the protection of personal data and access to information, it would be natural to add to it para. 6 devoted precisely to the IGPPD. There are no real obstacles for this useful and important State organ, serving the protection of human rights, to appear as a guarantor of our right to privacy, access to information, and even freedom of conscience and religion.

---

of the Law on the Protection of Personal Data, he/she orders discontinuance of further processing of the data or its removal (since Article 46 states that the processing may commence immediately after submitting an application, without waiting for the registration), and this is subject to immediate execution. Data processing may be resumed if the administrator's file has been registered, so the IGPPD has considerable supervisory powers. However, what happens if - 2. The administrator is under no obligation to register a data file due to its general availability (Article 43, para. 1, subpara. 9 of the Law on the Protection of Personal Data). At the same time and for the same reasons he/she does not inform the persons to whom the data pertains on the fact of processing it and does not provide other, usually obligatory, information (Article 25, para. 2, subpara. 2 thereof). Then, thanks to other subjects' ignorance, only the administrator can decide whether processing the data violates the rights and freedoms of the persons to whom the data pertains and whether he/she has done his/her utmost to ensure the protection of such persons' interests, in particular, whether the data is processed lawfully (Article 26, para. 1, subpara. 1). Such an administrator will see no reason in finding in this law the obligation to check the legality of the source of the data in question, limiting him/herself to meet the formal requirements expressed in the provisions of the law.