

Personal data protection under legal regulations

ABSTRACT

Contrary to appearances, personal data is a very extensive concept, which is included in the law both on the European and Polish. Today the term Specifies not only a name, but also other data that can be used to identify an individual. Consisting of four parts of the article raises very important questions about the same concept, European law and Polish and malicious activity relating to the misuse of such data. An in-depth analysis of the legal acts and an indication of the specific cases to bring all interested subject of protection of personal data. Article also contains a catalogue of risks associated with both deliberate administration of personal data loss and theft. This work is information and a warning-the goal is to increase awareness and alertness of our society. Making the society aware is an important issue, that many institutions are usually standing over the safety state of their data and of the organization.

Keywords: personal data, sensitive data, safety

1. Introduction

Every day there are numerous institutions, organisations, guards and inspections protecting the safety of all citizens. Nowadays, in the times of rapid changes taking place in every area of life, this requires a lot of work and involvement. However, the actions taken for personal data protection are not a sufficient means in the face of irresponsible activity of the society. Currently, people more or less consciously make available an increasing amount of information about themselves, e.g. through popular

social networks. These include very different data, because users state their names, surnames and provide several other basic data. We can also find there certain data which, under the existing legal regulations, can be considered as sensitive data, which are subject to special protection.

The problems of personal data security were legally regulated not only in the Constitution of the Republic of Poland, but also in the Personal Data Act of 29 August 1997, which has been effective for 20 years, despite many amendments. Inspector General for Personal Data Protection (IGPDP) is the body which governs personal data protection on a daily basis, and it is the activity of IGPDP that will receive particular attention in this article. IGPDP, acting on the basis of the legal regulations, is the contemporary guard of personal data security.

However, all actions taken both by the legislator and by IGPDP, are not a sufficient means to ensure one hundred per cent safety of citizens, because a majority of risks in this field are created by the society, which makes a lot of information about themselves available on a daily basis. This security is additionally reduced by fast development of information technology, Internet and any kinds of social networks. Therefore, among the specialists who handle issues related to personal data protection, there are increasingly frequent opinions about the need to adjust the regulations to the new reality.

2. Personal data and body responsible for their protection

Personal data is a term with very broad meaning, because the legislator did not create a closed catalogue of information which can be defined in this way. Instead, the Act contains a provision saying that *'personal data shall be understood as any information concerning an identified or identifiable natural person'* (Art. 6 of the Personal Data Act of 29 August 1997, Journal of Laws of 2016, Item 922). Due to this, a question arises – what type of information becomes personal data, is this a single piece of information, or a set of information? As explained by the Inspector General for Personal Data Protection, personal data shall not be understood as single pieces of information with a high degree of generality. They include e.g.. information such as:

- street name
- house number
- remuneration amount

However, such information will become personal data when provided with additional information thanks to which a particular natural person can be specified. An example of single piece of information, which is indisputably considered to be personal data is the PESEL number. In the light of Art. 15 of the Act of 24 September 2010 on population registration (Journal of Laws of 2016, Item 722), PESEL number is an eleven-digit numeric symbol which contains the date of birth, ordinal number and indication of gender.

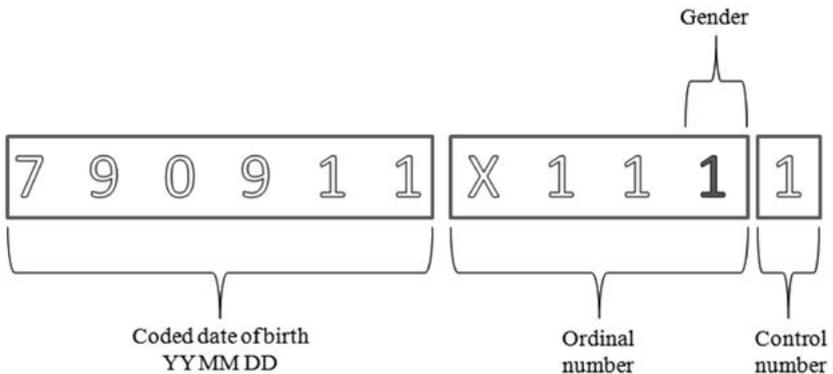


Fig. 1 Description of PESEL number pursuant to Art. 15 of the Act of 24 September 2010 on population registration.

PESEL number consists of elements such as:

- coded date of birth
- ordinal number
- coded gender
- check digit

Digits 0, 2, 4, 6, 8 – mean the female gender, whereas digits 1, 3, 5, 7, 9 refer to the male gender.

In fact, a city card number can also be regarded as personal data, unless establishment of such information generates a large amount of

costs, time and activities. Taking into consideration the fact that a city card contains a number linked to a particular person, assigned by an information system, an authorised carrier's employee is able to determine the owner of a card. The same applies in the case of e-mail address. If it contains information such as name and surname, or surname and company name, the owner can be determined without bearing any costs or excessive measures. It is different in the case when an e-mail address contains a general name and identification of the owner would require significant costs and work.

An example of e-mail address considered as personal data:

jan.kowalski@firmaabc.abc.pl

This address contains information such as: name, surname and name of the company represented by a particular person. Therefore, it is simple to determine the person indicated in the above address.

An example of e-mail address not considered as personal data:

potok@abc.pl

The word 'potok' in the above-mentioned address does not necessarily refer to a surname, location, and it can be a randomly selected word through which the owner cannot be determined easily.

In light of legal regulations, personal data are divided into common data, containing basic information, such as name, surname, PESEL number and sensitive data referring to religious or philosophical beliefs, any information containing ethnic and racial origin, as well as political beliefs and party affiliation. Sensitive data, specified in Art. 27 of this Act, also include medical data, i.e. data describing the health condition, as well as information on the genetic code. The current Act also classified as sensitive the information concerning any type of conviction, as well as penalty judgments, fines and judgments issued during administrative or judicial proceedings (Art. 27 of the Personal Data Act of 29 August 1997 with further amendments). The below diagram was created on the basis of Art. 6 and Art. 27 of the Personal Data Act in order to determine the basic division of personal data.

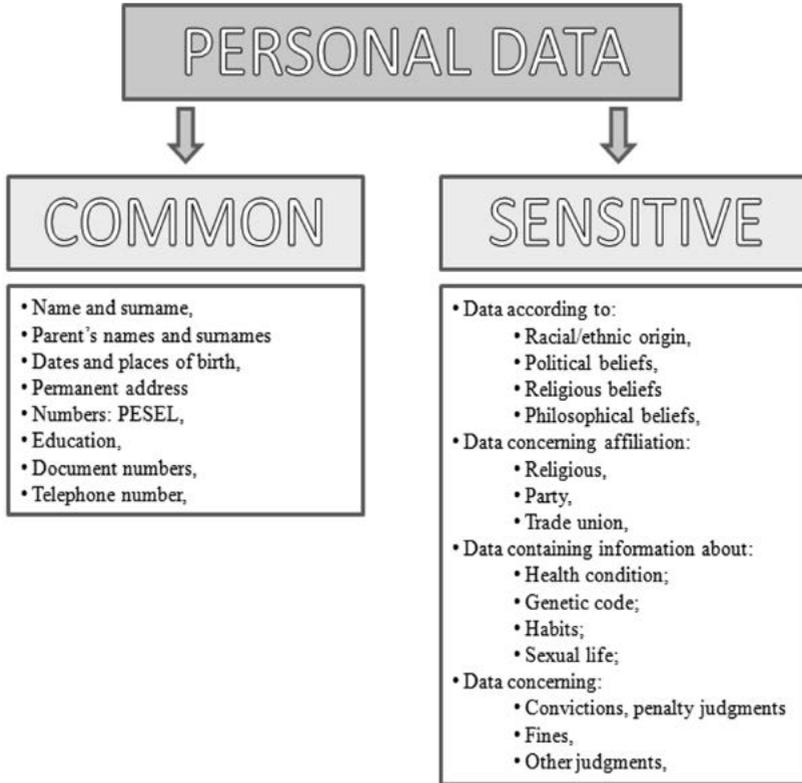


Fig. 2 Division of personal data in light of the Personal Data Protection Act of 29 August 1997.

The body responsible for personal data protection in the territory of the Republic of Poland is Inspector General for Personal Data Protection (IGPDP). Inspector General for Personal Data Protection is appointed and dismissed by the Sejm of the Republic of Poland (with the approval of the Senate) for a four-year term. However, they cannot perform their duties for more than two terms, i.e. 8 years. Upon the expiry of a four-year term, IGPDP shall perform their duties until their successor has assumed their position. The Act precisely defined that Inspector General for Personal Data Protection cannot take up work in a different position, with the exception of a professor of a higher education institution. In order to become Inspector General for Personal Data Protection, a person has to comply with all four statutory requirements included in Art. 8:

- be a Polish citizen and reside permanently in the territory of the Republic of Poland;
- be distinguished by high moral standards;
- have a higher legal education and relevant professional experience;
- have a clean criminal record (pursuant to Art. 8 of the Personal Data Protection Act of 29 August 1997).

This Act also specified the scope of activity of IGPDP. Therefore, acting on the basis of the applicable legal regulations, Inspector General for Personal Data Protection shall perform inspections in the field of appropriate data processing, compliant with the personal data protection regulations. IGPDP's task is also to maintain and provide information concerning registers of personal data, as well as registers of Administrators of Information Safety (AIS). Moreover, IGPDP shall provide opinions on draft acts and regulations concerning personal data protection, as well as participate in works related to this subject in domestic and international institutions. IGPDP shall also undertake a range of activities intended to increase the social awareness of the problem of personal data protection. Therefore, the IGPDP website contains valid legal acts, articles, publications, as well as information on conferences, courses and trainings. However, particular attention should be paid to the available information services, such as the educational and information website eduGIODO.

3. Personal data protection in the Polish legal system

Personal data security is guaranteed particularly by the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, no. 78, Item 483), in which the legislator focused on securing the most important interests of citizens. Art. 47 of the Basic Law stipulates that *'Everyone shall have the right to legal protection of their private and family life, of their honour and good reputation and to make decisions about their personal life.'* Therefore, activities such as collecting, processing and sharing personal data repeatedly affect the sphere of private life. In accordance with Art. 51 of the Constitution, every human being shall have the right to decide about disclosure of information concerning themselves. This means

that everyone can freely dispose of their own personal data. Also the provisions of the Constitution of the Republic of Poland clearly define that every human being shall have the right to access official documentation concerning themselves. A citizen cannot demand access to private collections and documents belonging e.g. to a collector. However, every human being has the right to demand their own data to be correct, and therefore, everyone has the right to correct or delete wrong data.

The Personal Data Act of 29 August 1997 (Journal of Laws of 1997 no. 133 Item 883) was adopted in the same year as the Constitution of the Republic of Poland, and work on this Act took as many as six years (Barta, Fajgielski, Markiewicz, 2011, 98 – 99). Taking into consideration that this Act did not have a predecessor, its authors faced a difficult challenge. *Directive 95/46/EC of the European Parliament and of 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* has become the basis of Polish regulations, and in consequence, a kind of model. The way from the moment of drawing up a draft act until its resolution was not a simple road. On 8 October 1996, two draft acts (one by the government and one by MPs) undertaking in detail the issues related to personal data protection were submitted in the Sejm of the Republic of Poland. The first reading of the draft acts was held on 20 November 1996, during the 94th session of Sejm, whereas the second reading took place on 30 July, and the third on 1 August. The voting results were as follows: 325 votes for passing the Act, 5 votes against and three MPs abstained from voting. The Act was eventually adopted during the 114th session of the Sejm of the Republic of Poland on 29 August 1997. A number of amendments have been introduced since then. A significant change in the Act was introduced on 25 August 2001, when the definition of personal data was amended. It was decided then that personal data do not only include the name, surname, VAT number or PESEL number, but also information that may serve to identify or ‘make it possible to identify’ a natural person. Moreover, the catalogue of sensitive data was extended by including fines and judgments of criminal proceedings (Kałużyńska – Jasak, 2013,124). The current Personal Data Protection Act consists of nine chapters. The first one of them begins with a very important sentence saying that *‘everyone has the right to protect their personal data’*, which refers to every natural

person. The first chapter is an introduction to the subject of personal data protection by explaining this term in Art. 6. It also defines the goals of this Act and rules of handling personal data, as well as responds to the fundamental question concerning the necessity of its application. The first chapter also contains a summary of basic terms in this field. The Act defines the principles of functioning of Inspector General for Personal Data Protection and their competences. In a large chapter dedicated to the rules of personal data processing, the legislator precisely determined in points when such data can be processed, as well as the role and importance of a personal data administrator. In Art. 27 of this Act, the legislator included a list of data which are subject to special protection (the so-called sensitive data). Although the term 'sensitive data' is not used in the Act, this notion is used with reference to information revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, religious, party and trade union affiliations, as well as data about health condition, genetic code, habits or sexual life and data on convictions, penalty judgments and fines, as well as other judgments of court or administrative proceedings. This Act also specifies the rules of providing personal data to a third party country and penal provisions in case of incorrect personal data use. Under this Act, the information concerning conceived yet unborn children, legal entities and organizational units without legal personality or deceased persons is not universally recognized as personal data. Due to this, relatives of the deceased may obviously demand that the information about the deceased will no longer be processed on the basis of the Civil Code with reference to personal data protection. The personal interest in this case is cult of the memory of the deceased (Szewc, 2007, 5). Based on IGDPD's interpretation, personal data shall be understood only as information about a natural person, i.e. a person who participates in legal relationships. The legal capacity of a human being is the capacity to be a holder of the rights and obligations. It is acquired at the moment of birth and ceases at the moment of death, or at the moment of being declared deceased. A person who has deceased or has been declared deceased cannot be a holder of rights and obligations, and therefore is not a party to any legal relationships, nor can they be recognised as a natural person. Therefore, the current Personal Data Protection Act shall apply only to processing personal data of living individuals.

The Personal Data Protection Act, amended several times, has been protecting the safety of personal data of all citizens for twenty years. A number of executive regulations to this Act have been issued. Data protection in IT systems is one of the most important issues in the times of dynamic changes and quick development of information technology. In order to secure data personal data in this field, relevant provisions had to be established to provide framework for such activities. *Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing (Journal of Laws of 2004, no. 100, item 1024)* is a kind of instruction concerning the rules of maintaining documentation related to personal data processing, as well as it determines the technical conditions of devices and IT systems intended for personal data processing. This document also contains a summary of key terms encountered by every person responsible for personal data protection. Here, particular attention was also paid to safety measures, taking into consideration division into basic, increased and high levels.

Another significant executive regulation is the *Regulation of the Minister of Internal Affairs and Administration of 11 December 2008 on specimen of a notification of a data filing system to registration by the Inspector General for Personal Data Protection (Journal of Laws of 2008, no. 229, item 1536)*, as the name suggests, containing a specimen of a notification of a set of personal data to IGPDP. Specimens of documents were also established in the *Regulation of the Minister of Administration and Digitization of 10 December 2014 on notification sample forms regarding appointments and dismissals of Administrator of Information Security (Journal of Laws of 2014, item 1934)*. The detailed guidelines for AIS are also included in the *Regulation of the Minister of Administration and Digitization of 11 May 2015 on the methods of running data register by Administrator of Information Security (Journal of Laws of 2015, item 719)* and *Regulation of the Minister of Administration and Digitization of 11 May 2015 on procedures and methods of implementing measures to ensure the observance of the regulations on personal data protection by Administrator of Information Security (Journal of Laws of 2015, item 745)*.

The status of the office of Inspector General for Personal Data Protection was established with the *Regulation of the President of the Republic of Poland of 10 October 2011 on granting the statutes to the Bureau of the Inspector General for Personal Data Protection (Journal of Laws of 2011, no. 225, item 1350)*. This document had been preceded by the Regulation of the President of the Republic of Poland of 3 November 2006 on granting the statutes to the Bureau of the Inspector General for Personal Data Protection (Journal of Laws no. 203, item 1494), which, however, expired on 7 March 2011 pursuant to Art. 1 Item 3 Letter b of the Act of 29 October 2010 amending the Act on the Protection of Personal Data and certain other acts (Journal of Laws no. 229, item 1497). The Regulation of 2011 (Journal of Laws of 2011, no. 225, item 1350) determines the organisational structure of the Bureau of the Inspector General for Personal Data, as well as its location and branches. There were also amendments in 2015, as specified in the *Regulation of the President of the Republic of Poland of 19 November 2015 amending the regulation on granting the statutes to the Bureau of the Inspector General for Personal Data Protection (Journal of Laws of 2015, item 2020)*.

The fast approaching reform of personal data protection has already given rise to many concerns. In May 2016, texts of the following legal acts were published in Official Journal UE L 119:

- Directive 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Council Framework Decision 95/46/EC.
- Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

The need to create new regulations in the field of personal data protection is motivated by the dynamic development of information technology and the already universal use of Internet almost in every area of life. Nowadays,

the Internet has revolutionised the manner of communication, therefore becoming an inseparable part of life. Due to the universal use of this means of communication, the currently effective legal regulations have become obsolete to some degree. It does not mean that they completely lost their protective functions; however, they fail to cover many important aspects. The changes planned for 2018 are highly required, because Directive 2002/58/EC refers to traditional telecommunications operators, whereas the new regulations will also cover new means of communication, including online telephony, e-mail and Instant Messaging services. Also Facebook, ranked among the most popular social networks, will have to apply the new regulations.

4. Conclusion

Without any doubt the new reality and dynamic changes that we have to face each day required the legislator to introduce changes in the field of personal data protection. The previous regulations were created in the times before Facebook, when the Internet did not play such a significant role. New regulations also mean new challenges, both for IGPD and all administrators of information security, and they are expected to come into force from May 2018.

Every human being deals with personal data when performing daily duties. The regulations of current Personal Data Protection Act are applied during conclusion of agreements, recruitment process for a particular job position, as well as creation of a social network or e-mail account. Frequently repeated actions are becoming a standard to such a degree that we gradually attach less importance to the problem of personal data security. This happens e.g. in virtual reality which attracts many users, giving them opportunities they had never had before. Nowadays, through social networks, every user can manifest themselves and show their best side, frequently marginalizing the safety rules and abandoning the right of privacy to which they are entitled. Such activities are related to disclosing personal data and photos which may in the wrong hands become a tool for committing a crime.

The primary goal of personal data security specialists is to make society aware that every citizen is entitled to personal data protection; however,

only reasonable use of various means of communication guarantees safety. The best form of security for citizens is reasonable actions and taking care of their own data.

Bibliography:

- Barta J., Fajgielski P. (2011). Markiewicz R., *Ochrona danych osobowych. Komentarz*. Wydanie 5, Warszawa.
- Kałużyńska – Jasak M. (2013). *15 – lecie ustawy o ochronie danych osobowych*, Warszawa.
- Szewc T. (2007). *Publicznoprawna ochrona informacji*, Warszawa.

Legal acts:

- Directive 95/46/EC of the European Parliament and of 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.
- Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
- Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, no. 133, item 883)
- Regulation of the Minister of Internal Affairs and Administration of 29 April 2004 as regards personal data processing documentation and technical and organisational conditions which should be fulfilled by devices and computer systems used for the personal data processing (Journal of Laws of 2004, no. 100, item 1024).
- Regulation of the Minister of Internal Affairs and Administration of 11 December 2008 on specimen of a notification of a data filing system to registration by the Inspector General for Personal Data Protection (Journal of Laws of 2008, no. 229, item 1536).
- Regulation of the Minister of Administration and Digitization of 10 December 2014 on notification sample forms regarding appointments and dismissals of Administrator of Information security (Journal of Laws of 2014, item 1934).

- Regulation of the Minister of Administration and Digitization of 11 May 2015 on the methods of running data register by Administrator of Information Security (Journal of Laws of 2015, item 719)
- Regulation of the Minister of Administration and Digitization of 11 May 2015 on procedures and methods of implementing measures to ensure the observance of the regulations on personal data protection by Administrator of Information Security (Journal of Laws of 2015, item 745).
- Regulation of the President of the Republic of Poland of 10 October 2011 on granting the statutes to the Bureau of the Inspector General for Personal Data Protection (Journal of Laws of 2011, no. 225, item 1350).
- Directive 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Council Framework Decision 95/46/EC.
- Regulation of the President of the Republic of Poland of 19 November 2015 amending the regulation on granting the statutes to the Bureau of the Inspector General for Personal Data Protection (Journal of Laws of 2015, item 2020).
- Personal Data Protection Act of 19 August 1997 (Journal of Laws of 2016, item 922).
- Act of 24 September 2010 on population registration (Journal of Laws of 2016, item 722).

