Protection of the personality rights and personal data

Piotr Woglowski
Publication concept:
Paweł Skowera

Author:
Piotr Waglowski

Publisher:
Polish Agency for Enterprise Development (PARP)
ul. Pańska 81/83, 00-834 Warszawa

www.parp.gov.pl

Typesetting:
Marcin May PARP

1st edition
Complimentary publication

The publication has been produced under the project entitled: “Launch of a multifunctional platform for web-based communication to support the implementation of OP IE 8.1 and 8.2 Measures”, which is being implemented by the Polish Agency for Enterprise Development and has been granted co-financing by the European Union under the European Regional Development Fund.

We support e-Business www.web.gov.pl

Copyright © by Polish Agency for Enterprise Development (PARP), Warsaw 2009.

All rights reserved. No part of the publication may be used in any form, nor may it be translated to mechanical language without prior consent by PARP.
Contents

1. Personality rights .................................................................................................................. 4
   1.1. Open catalogue of personality rights in the “information society” ............................. 5
   1.2. Privacy .............................................................................................................................. 6
   1.3. Protection of the personality rights ............................................................................. 8

2. Protection of personal data ................................................................................................. 9
   2.2. The term of personal data .............................................................................................. 10
   2.3. Data processing ............................................................................................................ 11
   2.4. Information obligation .................................................................................................. 13
   2.5. Organisational and technical matters of data processing ........................................ 14
   2.6. Data processing security levels ..................................................................................... 15
   2.7. Personal data in certain legal acts ................................................................................ 16
1. Personality rights

The personality rights are enjoyed by all natural persons. They are non-material, they cannot be transferred (they are non-tradable), they cannot be waived, and they expire upon death of the holder of the right. The Civil Code presents an exemplary catalogue of such rights: health, freedom, honour, freedom of conscience, surname and pseudonym, image, secrecy of correspondence, inviolability of home premises, scientific work, arts, inventions and rationalisation measures. These rights are protected by the civil law irrespective of the protection granted on the basis of other regulations. An open list of the personality rights increases e.g. as a result of court jurisprudence. Apart from the indicated catalogue, it also covers the personality rights pertaining to the area of private and family life and intimacy. As decided upon by the Supreme Court: protection in this respect may refer to the cases in which facts were disclosed from private and family life, abuse of obtained information, collection of information from private interviews and intimacy assessments in order to publish them or disseminate in another way. This is why, privacy is a personality right of a human.

The personality rights are enjoyed accordingly by legal persons as well. The term “accordingly” means that legal persons are not protected the same way as natural persons. A legal person, for instance, does not have an image, which – to put it simply – represents what can be registered (image is almost an equivalent of a picture, drawing of a given natural persons, sometimes it applies to other image types, e.g. when we register somebody’s utterance). The Supreme Court decided that the image of a legal person is not represented by the image of a place where it has its seat or the images of persons composing its bodies or even the entire team and similar elements (considered separately or jointly). Similarly, health of a legal person is out of question too. Within another meaning, the Court decided that personality rights include “the non-material values owing to which a legal person can function in accordance with its scope of activity”.

Protection of personality rights covers both the protection in case of infringement of rights, but also in case of threat to them (in the event of threat of the personality rights, can one also exercise the rights provided for by the Code). However, the vested protection can be exercised solely in case of illegal threat or infringement. There are some circumstances that exclude illegality. In this context, one can speak of consent by the right holder, measure based on a legal provisions or measure implementing individual rights, measure to protect justified public interest. A measure threatening or violating somebody’s individual rights can also consist in an act of omission. In addition, it should be kept in mind that illegality of the act that infringes a personality right is implied (in consequence, it should be assumed that the persons that violates a given personality right has to prove in case of a dispute that their actions were not illegal).

A personality right should correspond to the interests of an average human being and be objective, meaning that when assessing an infringement of for instance

---

2 Judgement of the Supreme Court, Civil Chamber of 25 May 1977, ref. No.: I CR 159/77
3 Judgement of the Court of Appeal in Warsaw of 19 December 1995, ref. No.: IACR 1013/95
honour, one should take into consideration not only the subjective feeling of
the persons claiming legal protection, but also the objective response in the public
opinion⁴.

1.1. Open catalogue of personality rights in the “information society”

Nearly all personality rights listed in the Codex catalogue can be threatened or
infringed in the Internet (only maybe apart from the inviolability of home premises).
Flickering graphics on a web forum that is frequently used by persons suffering from
epilepsy may result in the death of such persons, and it is for sure a threat to their
health. Freedom is also understood as freedom from anxiety and fear, from
violence or execution of threats of another person.

Publications in the Internet may result in the violation of honour (that is both good
name and personal dignity): in such a case, additional protection is provided by the
provisions of the Penal Code, which provide for a penalty for slander in the means
of mass communication. The right to surname can be infringed too (for instance by
illegal placement of such a surname in the name of a domain). In the context of
the Internet, a new meaning is given to the protection assured for a pseudonym.
As pointed out by the Supreme Court⁵: “a user name used by a person who uses
the Internet is subject to legal protection on the same basis as is the case for
protection of a surname, pseudonym or firm”. Infringement of the right to image
covers e.g. the publication of somebody’s photograph without their consent.
The protection of the image is additionally supported by the provisions of the
copyright law: consent to dissemination of image has to be granted by the person
presented therein, but it does not apply to commonly known persons or the ones
that are only a small part of an entity, such as for instance a meeting.

In relation to the above-mentioned comments, one of the first decisions of Polish
courts of law on the application of “links” should be mentioned. As pointed out by
the Court of Appeal in Kraków⁶: “The circumstance that the defending party had no
impact on the content of webpages to which they sent the portal users is not
important for the evaluation of their responsibility for infringement of
the complainant’s personality rights. This responsibility is connected with publishing
on the portal of the defendant’s website a reference (link) to the webpage where
the image of the claimant was published and with recommendation of this webpage
by the defendant, and not with the introduction of this website to the Internet
and formulation of its content”.

Protection of correspondence, and even “communication” is obvious.
The protection of such a right – in connection with ever growing use of the Internet –
appears to be more and more significant. Browsing of somebody’s electronic mail,
its publication in the Internet without relevant authorisation may represent a threat to
such personality right, beside the threat to privacy.

It should be kept in mind that creative work, as such, is also a personality right that
is covered by protection under the Civil Law. At this point, the thesis of the Court of

---

⁴ Judgement of the Supreme Court of 16 January 1976, ref. No.: II CR 692/75, OSN 1976/11/251
⁵ Judgement of the Supreme Court of 11 March 2008, ref. No.: II CSK 539/07.
⁶ Judgement of the Court of Appeal in Kraków of 20 July 2004, ref. No.: I ACa 564/04.
Appeal in Warsaw\textsuperscript{7} should be mentioned in which it decided that “for the legal protection of author’s rights to a work, it does not matter how the person committing the infringement came into possession thereof or how they obtained the work, in particular it does not matter that the creative work that is the object of infringement reached the person committing the infringement as unwanted correspondence sent via electronic means, commonly referred to as spam”. This specific dispute pertained to a work – a poem – that was not ordered, but sent to the editorial team who afterwards published it. In the same decision, the Court also acknowledged the protection of such authors that are anonymous for the entity infringing their rights: “Protection covers not only a commonly known author, whose works are published in large circulation, but every author whose rights to a work were violated in any way whatsoever, the right enjoyed by the author”. This thesis may be of major importance for all persons who would like to use the works they found in the Internet, but do not know anything of the authors.

In the case of natural persons and legal persons, it is the firm that is in question, meaning the label under which an entrepreneur operates. In the case of natural persons, as a rule, it will be the name and surname, if need be along with additional marks such as e.g. identification of the area of business; in the case of legal persons, it will be their name containing additionally the specification of the legal form in it. According to the jurisprudence, “the firm under which a given entity operates its business has such a meaning in the entered legal relationships as a surname for a natural person”\textsuperscript{8}.

\textbf{1.2. Privacy}

A personality right that is not provided for in the Codex catalogue is privacy. It deserves extraordinary emphasis in this study due to the development of the “information society”, whose members gain ever growing technical opportunities to intervene in this right. The protection of the right to privacy is governed in a very extensive way. The provisions on the right to privacy are included in international agreements on human rights, e.g. the European Convention on Human Rights, they are also included in the European Union law, in the Constitution of the Republic of Poland and in a number of detailed Acts of Law, for instance in the Press Law. Civil-law protection of the right to privacy, as the human's personality right, is also accompanied by administrative and legal protection of personal data (that is handled in a separate chapter in this study). In addition, support for protection of privacy is provided by certain provisions of the Penal Law.

As regards the right to privacy as the main human right, a reference should be made to Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) that indicates that each person enjoys the right to respect for their private and family life, their home and their correspondence. At the same time, this provision introduces the principle according to which it is inadmissible for public authorities to intervene in exercise of the above-mentioned right, with the exception of cases provided for in the Act and necessary in a democratic society due to the national security, public security and country's

\textsuperscript{7} Judgement of the Court of Appeal in Warsaw of 14 March 2006, ref. No.: VI ACa 1012/2005.
\textsuperscript{8} Judgement of the Court of Appeal in Poznań of 22 October 1991, ref. No.: I ACr 400/90
economic prosperity, protection of order and prevention of crime, healthcare, protection of morality or protection of human rights and freedoms. Therefore, the right to privacy can be restricted, provided that a number of conditions are met.

With regard to this provision, the judgements of the European Court of Human Rights have been passed that should be referred to in the context of protection of privacy in an “information society”. The Court decided for instance that Article 8 of the Convention was violated in the case in which monitoring of a female employee of a British university was examined (it was determined during the trial that the monitoring consisted, inter alia, in verification of websites visited by the employee, the dates and duration of these visits of these websites were analysed, the monitoring also covered the activity connected with the use of electronic mail by her)9.

The provisions of the Constitution of the Republic of Poland provide for a number of provisions that concern privacy. These provisions form the basis for further regulations in this respect in the provisions at the level of acts of law. However, it should be kept in mind that it is precisely the Constitution where the right to legal protection of private life, honour, good name and the right to determine one’s private life were introduced; it also contains the guarantees of the freedom to communicate and protection of secrecy of communication, guarantees of the freedom to express opinions and to obtain and disseminate information, as well as the guarantees to consumer protection against the actions threatening their privacy.

As mentioned in the first part of this study (cf. Chapter 1.4), the problems concerning the protection of privacy appears in a number of legal acts of the European Union law as well.

In consequence of numerous regulations on the right to privacy, the provisions on this area are also included in the provisions at the level of acts of law, which cover the Press Law, the Telecommunication Law, the Act on combating unfair competition and the Act on provision of services via electronic means.

Privacy is a human personality right, and it is subject to protection on the basis of the Civil Code provisions. It is justified in the settled jurisprudence of the Supreme Court and other courts of law. Pursuant to the decision of the Supreme Court10 most essential for these problems: “The open catalogue of personality rights (Article 23 and 24 of the Civil Code) also covers the personality rights that are related to the area of private and family life and intimacy. Protection in this respect may refer to the cases in which facts were disclosed from private and family life, abuse of obtained information, collection of information from private interviews and intimacy assessments in order to publish them or disseminate in another way.

The problems concerning the protection of privacy begin to emerge in the court rulings that pertain to the “information society” in the broad sense. A judgement of the Court of Appeal in Warsaw11 should be mentioned at this point in which sending short messages (SMS) to a former associate constituted an infringement of the right

9 Judgement of the European Court of Human Rights of 3 April 2007 in the case Copland v. the United Kingdom (no. 62617/00)
10 Judgement of the Supreme Court, Civil and Administrative Chamber of 18 January 1984, ref. No.: I CR 400/83, OSNCP 1984/11 item 195
11 Judgement of the Court of Appeal in Warsaw of 2007, ref. No.: I ACa 584/06.
to privacy in this specific case. In the case, it was of major importance that the messages were being sent over a longer period, although the phone subscriber demanded that this illegal activity be discontinued, the senders did not satisfy this request; the messages “were supposed to mobilise to activity” despite the fact that the persons receiving them (some of them were received at 5 or 6 am) did not cooperate with the sending entity at that time. Such verdicts also form the basis for the formulation of a thesis that on the basis of the provisions on the protection of personality rights, in particular the right to privacy, it is possible to combat the problem of dispatch of unwanted electronic mail (meaning the “spam”; these problems will also be touched upon in the considerations on the basis of regulations on provision of services via electronic means in the further part of this study; cf. Chapter 4.3.5).

1.3. Protection of the personality rights

The regulations provide for both the non-material means of protection of the personality rights and the material means of protection. The non-material means of protection include for instance the demand to discontinue the measures that threaten personality rights (provided that it is illegal). Demand to take measures necessary to make good the effects of infringement is also a personality right (in particular declaration of appropriate content and form, but not only that since it is imaginable that in the case of violation in the Internet such measures will be constituted e.g. by provision of a dedicated file containing an instruction on the server for search engines to remove the given Internet resource from search results). The Civil Code also provides for other cases when non-material means of protection can be applied. They include for instance an action for declaration of illegality of infringement.

The material means of protection include, for instance, the right to be awarded financial compensation or payment of a specific amount of money for an indicated social purpose. The aggrieved party is allowed to claim damages on a general basis provided for in the Civil Code, which is possible in case when as a result of violation of a personality right, material damage was incurred.

Apart from the regulations included in the Civil Code, other provisions also contain additional means of protection of personality rights (e.g. the previously discussed Act on copyrights and related rights).

At this point, we should mention certain verdicts that were related to the violation of personality rights in press activity. For instance, the Supreme Court decided that non-material claims connected with infringement of a personality right in a press material may be lodged against a publisher as well, and the basis for such claims will be formed by the provisions of the Civil Code. In another verdict, the Supreme Court decided that “referring to a publication or utterance of another person can – in the circumstances of a specific case – turn out to be insufficient to refute the accusation of absence of illegality of the infringement of personality rights”.

Finally, a judgement should be mentioned that was passed on the basis of provisions of Press Law in reference to personality rights. The Court of Appeal in

---

12 Resolution of the Supreme Court, Civil Chamber of 7 December 1993, ref. No.: III CZP 160/93.
13 Judgement of the Supreme Court, Civil Chamber of 28 May 1999, ref. No.: ICKN 16/98.
Katowice decided\(^{14}\) that “media are obliged to respect values such as human personality rights. Freedom of speech does not mean the freedom to use it. The limit for the freedom to use the freedom of speech is defined by Article 12 of the Press Law, which obliges the journalists to exercise due diligence and honesty when collecting and using press material, notably to verify the accurateness of obtained information or to quote the source for it”. Such verdicts on the functioning of the media are extremely numerous, and above only several were mentioned to illustrate the importance and diversity of forms of protection of personality rights.

2. Protection of personal data

The problems concerning personal data protection is governed in Poland by the provisions of the Constitution of the Republic of Poland (e.g. in the scope of the right to privacy), the Act of 29 August 1997 on personal data protection (in the case of this Act, particular attention should be put on a number of implementing act that are of major importance due to fulfillment of the obligations arising from the personal data protection), the Act of 18 July 2002 on provision of services via electronic means, the provisions of a number of specific acts of law. At the level of the European Union, \textit{inter alia} in such legal acts as 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 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector and 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).

As far as constitutional norms are concerned, apart from legal protection of private life and determining one’s own personal life, the Constitution stipulates that the obligation to disclose the data on a specific person has to result from the Act, and the bodies of public authorities may process only the personal data that are necessary in a democratic state. At the same time, the Constitution gives a citizen the right to access to the data that pertain to them, to correct or to remove the data that apply to them and are incorrect, incomplete or collected in breach of the provisions of the Act.

2.1. The Act on personal data protection and the implementing acts

The Act on personal data protection regulates: the rules of procedure in personal data processing, the rights of natural persons whose data are or can be processed; it also introduces the protection rules for the processing of personal data, the procedure for registration of personal data, the procedure for submission of personal data to third parties and penal sanctions concerning the infringement of the Act on personal data protection. In addition, the Act establishes the Inspector

---

\(^{14}\) Judgement of the Court of Appeal in Katowice of 4 November 1999, ref. No.: I ACa 536/99.
General for the Protection of Personal Data\textsuperscript{15} as the chief personal data protection body and defines its competences.

Implementing acts have been issued for the Act on personal data protection, and they have to be taken into account as well when analysing the obligations and rights arising from the Act:

- Ordinance of the Minister of Interior and Administration of 29 April 2004 on the documentation for personal data processing and technical and organisational conditions to be met by the devices and IT systems used to process personal data\textsuperscript{16},
- Ordinance of the President of the Republic of Poland of 3 November 2006 on the award of statute to the Office of the Inspector General for the Protection of Personal Data\textsuperscript{17},
- Ordinance of the Minister of Interior and Administration of 29 April 2004 on the model registration data submission to the Inspector General for the Protection of Personal Data\textsuperscript{18},
- Ordinance of the Minister of Interior and Administration of 22 April 2004 on the model authorisation by name and official identity card of the Inspector General for the Protection of Personal Data\textsuperscript{19}.

Apart from the Act on personal data protection and the previously discussed Civil Code regulation on personal data protection, the provisions on personal data protection have also been included in other legal acts. What is important, however, is that pursuant to the Act on personal data protection, in case when special provisions provide for protection that goes beyond the scope arising from the Act, precisely these special provisions should be applied.

2.2. The term of personal data

Personal data applies to any information on an identified or identifiable natural person. Pursuant to the Act on of personal data protection, an identifiable person is a person whose identity can be defined directly or indirectly, in particular by means of an identification number or one or several specific factors specifying their physical, physiological, mental, cultural or social features. A piece of information is considered incapable of defining the identity of a given person if it would require excessive costs, time or effort.

Personal data comprise both the data that make it possible to define the identity of a specific person, as well as the data that, with the certain investment of funds, time and effort, are sufficient to determine it, although they do not allow for it to be immediately identified. Personal data cover such data that enable the determination of identity of a given person without extraordinary effort and costs, in particular by means of easily available and commonly accessible sources. Personal data do not include individual pieces of information of high level of generality. Depending on

\textsuperscript{15} http://www.giodo.gov.pl.
\textsuperscript{16} Dz.U. of 2004, No. 100, item 1024.
\textsuperscript{17} Dz.U. of 2006, No. 203, item 1494.
\textsuperscript{18} Dz.U. of 2004, No. 100, item 1025.
\textsuperscript{19} Dz.U. of 2004, No. 94, item 923.
the occurrence in connection with other pieces of information, a piece of information of high level of generality will represent a personal datum when it is listed with other additional information that allows for a specific person to be identified. For instance a PESEL number (personal ID) is a single piece of information that constitutes personal data.

In one of the decisions that applied to the data made available by the users of the nasza-klasa.pl website and concerning the plaintiff, the Inspector General for the Protection of Personal Data questioned the recognition of information on name and surname of the plaintiff as personal data in connection with the information on the name and address of the primary school and designation of the grade attended by them along with their image of 1978/1979, and it was decided that: "the analysis of the presented facts leads to the conclusion that the possibility, if any, of connecting the above-mentioned sequence of information about the plaintiff with them at present requires the use of disproportional costs, time and effort. It should be also pointed out that the plaintiff's name and surname were attributed to their image from years ago by a third person in form of a comment of a photograph, and in this sense, this piece of information is not of objective nature". GIODO also publishes court verdicts that pertained to the decisions previously issued by it on the website maintained by them, as well as other materials making it possible to interpret the Act.

Personal data can be divided into regular personal data and sensitive personal data. The provisions of the Act on personal data protection have introduced prohibition for certain data categories on the processing thereof (although they provide for a closed list of situations in which it will be admissible to process them at the same time). The catalogue of sensitive data is a closed catalogue and covers:

- racial and ethnic origin,
- political opinions,
- religious or philosophical belief,
- religious affiliation or party or trade-union membership,
- data on health condition,
- genetic code,
- addictions,
- sexual life,
- data on the convictions, verdicts on penalties and fines and other decisions issued in judicial or administrative proceedings.

2.3. Data processing

The Act defines the term personal data protection and understands it as any operations conducted in relation to personal data, such as collection, saving, storage, elaboration, modification, provision of access and removal, and in particular

---

the operations that are carried out in IT systems. The Act does not define
the individual forms of data processing (with one exception), and hence their proper
dictionary definitions should be used. An extraordinary form of data processing is
represented by removal of data. Removal of data is one of the forms of processing
that does not require the consent of the persons to whom they apply. Removal of
data covers:

- destruction of personal data, meaning – depending on the data storage
  medium on which they are saved – the destruction of the data storage
  medium itself or, in case of the media used in IT systems, deletion of saved
  data,

- modification to the degree that prevents the identification of a person to
  whom the data apply, meaning a change in the data to the condition
  in which the determination of identity of a natural person would require
  excessive costs, time or effort.

The Act on personal data protection applies to personal data that are or can be
processed in data collections. Processing of personal data found in a collection is
an exception, provided that the processing takes place in an IT system (certain
exceptions are provided for by the Act on provision of services via electronic
means). A collection, within the meaning of the Act, is constituted by “any structured
set of personal data that are available according to specific criteria, irrespective of
whether such a set is functionally dispersed or separated”.

A data collection is subject to submission for registration purposes to
the Inspector General for the Protection of Personal Data with the exceptions that
arise directly from the provisions of the Act. Such an exception covers e.g.
the collection of personal data that are processed because of employment at the
data administrator (i.e. the collections on the current and past employees, as well as
the candidates) and the provision of services for the data administrator on the basis
of civil law contracts (e.g. on the basis of contracts of commission or contracts for
specific work). The provisions exempting from the obligation to register collections
do not exempt an administrator from other obligations, such as for instance to take
security means necessary under the law in relation to data processing and the obligations to provide information.

Data processing also entails the term of data administrator, that is e.g. a body of
an organisational unit and certain other entities listed in the Act that decide
on the purposes and means of data processing. An administrator of personal data
used in the area of business conducted by an entrepreneur is the entrepreneur
themselves, and not the bodies thereof or natural persons sitting on the bodies of
the entrepreneur. A data administrator is in particular a limited liability company,
a joint-stock company, a general partnership or a limited liability partnership. In case
of economic activity conducted by a natural person, the person conducting
the economic activity is the data administrator. They remain the data administrator
even if a person responsible for processing of personal data is designated. In case
of assignment of data for processing to an external entity, the entity submitting these

---

21 The obligation is lifted in the case of administrators of data collections listed in
the provision of Article 43(1) of the Act on personal data protection.
data remains the data administrator, and they are still responsible for fulfilment of all obligations arising from the Act despite assignment of data.

One of the premises allowing for data to be process is **the consent by a person to whom they apply.** Consent to personal data processing must not be implied or alleged from a declaration of will with other contents. Personal data processing is admissible solely when the person to whom the data pertain has granted consent to it (personal data processing consisting in removal of data that concern such a person is an exception). The contents of the declaration of will on granting consent to personal data processing should indicate that the person who grants consent does so while being fully aware of the purpose, scope and processing person of the personal data processing. Granting consent to data processing may also cover the processing in the future, in so far as the purpose of processing does not change. Consent to data processing, granted in writing by the persons to whom the data apply, represents one of the conditions that make it possible to process “sensitive” data.

### 2.4. Information obligation

Submission of information about the processing of personal data is covered by one of the obligations imposed on an entity that process personal data (data administrator). The data undergoing processing can be obtained by a data administrator in two ways: directly from the person to whom the data apply and from a third entity. Should the processed data not come directly from the person to whom they apply, the entity that processes the data (data administrator) is additionally obliged to inform about the source (origin) of processed data.

The information obligation arises once the personal data have been collected. This means that directly after the data have been saved by the processing entity, the person to whom the data pertain enjoys the right to obtain information about the name and address of the seat of the processing entity, the purpose of data collection and scope thereof, the rights of the persons in relation to processing, i.e. the right to access to data and the right to correct them, as well as the freedom or obligation to submit the data (in case of applicable obligation to submit the data, the legal basis for application of such an obligation should be indicated). In case when the data were obtained not from the person to whom the data pertain, the information about the source from which it was derived should be indicated as well. Failure to meet the information obligation can be represent the grounds to lodge a complaint to the Inspector General for the Protection of Personal Data by a person who has not obtained information in this respect.

The scope of information obligation covers additionally the obligation for data administrator to submit the information on the rules for personal data protection. Such information is submitted by data administrator upon request of the person whose data undergo processing. This obligation arises from the right of the person whose data undergo processing to control the processing of such data. Within 30 days of the submission of application by the person whose data undergo processing, the administrator has to provide an answer containing information about: the presence of personal data collection, data administrator – as regards its name and registered office address (in the case of natural persons – name and surname and address), the purpose, scope and method of processing of
the data included in a collection, the date of commencing the processing of data concerning the applicant, the contents of such data, submitted in a comprehensible form, the source of such data (with the exception of validity of statutory secrecy in this respect applicable to the administrator), the provision of such data, in particular about the recipients or categories of recipients to whom the data are made available. Failure to fulfil the information obligation might result in administrative and legal responsibility before the Inspector General for the Protection of Personal Data and penal responsibility.

2.5. Organisational and technical matters of data processing

A data administrator is obliged to use technical and organisational means that, depending on the category of processed data and threats, will assure proper protection of process data. A data administrator maintains the documentation that describes the method of data processing and the measures taken to protect the data. A data administrator should protect the data in particular against:

- provision of access for unauthorised persons,
- being taken by an unauthorised person,
- processing in breach of the Act,
- modification, loss, damage or destruction.

Only the persons authorised by a data administrator may be provided access to data processing. An administrator is obliged to keep records of the persons authorised to processing of personal data. They are also obliged to assure control over who and when has introduced the data into the personal data processing system, what the introduced data are and to whom they are submitted.

Pursuant to the Ordinance of the Minister of Interior and Administration of 29 April 2004 on the documentation for personal data processing and technical and organisational conditions to be met by the devices and IT systems used to process personal data, the documentation kept by a data administrator that describes the data processing method and the measures taken to protect them include: security policy and instruction on management of the IT system used to process personal data.

**Security policy** should cover all the aspects of protecting the personal data (both the data processed in IT systems and the ones processed in a traditional way). As part of preparing the security policy, an administrator can attribute the scope of duties connected with the personal data processing to individual persons and define: the personal data resources, processes important for the sustainability of functioning of the data administrator (in connection with personal data processing), threats that have impact on the protection of processed data, susceptibility of the IT system to threats, protection measures for the personal data processing (in an IT system and beyond such system), the risk present after implementation of protection mechanisms. The security policy for personal data processing should contain, among other things, the specification of the area of personal data processing by means of a list of buildings, rooms, room parts in which such data are processed (irrespective of whether processing is conducted in a traditional way or in an IT system), a list of personal data collections.
and the specification of programmes used to process the data, the description of structure of data collections to indicate the contents of individual information fields and interrelations between them, the method for transfer of data between individual systems, the specification of technical and organisational means necessary to assure data confidentiality, integrity and accountability (i.e. the possibility to attribute entity’s measures in an unambiguous manner solely to that entity).

The term of instruction on management of the IT system serving the purpose of personal data processing can be used to refer e.g. to the procedure for award of IT system identification to a user or award of rights to process information, methods and means to authenticate the users of such a system, the procedure for creation of backups, etc. The instruction can also contain the procedure for a situation when a violation in the security of the IT system used to process personal data is detected.

The above-mentioned documentation is kept (in writing) and implemented by a data administrator. Implementation is to be understood as publication of documentation and getting acquainted with it by the persons authorised to process personal data and the persons that might have impact on the security of data processing. A data administrator should also organise training for the persons authorised to process personal data in the matters contained in the security policy and the instruction.

2.6. Data processing security levels

Ordinance of the Minister of Interior and Administration of 29 April 2004 on the documentation for personal data processing and technical and organisational conditions to be met by the devices and IT systems used to process personal data introduces 3 levels of data processing security means in the IT systems.

Basic level is applied when the IT system is not used to process “sensitive” data, and when no devices belonging to the system are connected to the public network. Such a system uses the following security means:

- The area in which personal data are processed is protected against access of unauthorised persons; unauthorised persons may be present within this area solely when consent has been granted by the data administrator or in the presence of an authorised person;
- The IT system for personal data processing is fitted with mechanism for control of access to the data;
- The IT system serving the personal data processing is protected against the programmes that are aimed at unauthorised access to the IT system and data loss caused by power supply failure or disturbance in the power supply network;
- The identification of a user who has lost the data processing rights must not be assigned to another person;
- In case when passwords are used for user authentication, a change thereof takes place at least every 30 days; the password consists of at least 6 symbols;
- The personal data processed in the IT system are protected by means of backup copies of data collections and programmes serving the data.
processing; the backup copies are stored in a place that protects them against unauthorised take-over, modification, damage or destruction, and they are deleted immediately when their utility has expired.

In case when "sensitive data" are processed in an IT system, but there are still no devices within the system that are connected to the public network, the medium level shall apply, in which the following measures should be taken apart from the measures provided for in the case of the basic system:

- User authentication password should consist of at least 8 symbols;
- The devices and data storage media containing the data are protected in a method that guarantees their integrity and confidentiality.

High level is used when at least one device of the IT system used to process personal data is connected to the public network. With such a security level, such measures should be taken that are used at the basic and medium level and additionally the following:

- The IT system serving the personal data processing is protected against threats originating in sources outside the public network by means of implemented physical or logical protection means against unauthorised access;
- In case when logical protection measures are taken, they cover the control of information flow between the data administrator's IT system and the public network and control of the measures initiated from the public network and the data administrator's IT system;
- The data administrator takes the cryptographic protection measures for the data used for authentication and transferred within the public network.

2.7. Personal data in certain legal acts

The regulations on the personal data protection can also be found in numerous other separate acts of law. The above-mentioned selected ones do not deplete the list of such acts of law, and it is presented only as an example.

The Act of 26 June 1974 – the Labour Code – stipulates that an employer has the right to request that the person applying for a job submits personal data covering: name(s) and surname, names of the parents, birth date, place of residence (mailing address), education, history of previous employment. An employer has the right to request that an employee also submits their other personal data, as well as the names and surname of their children and dates of their birth if submission of such data is necessary due to the employee’s use of special rights provided for in the Labour Law. They are also entitled to request the employee's PESEL number. Submission of personal data to an employer is made in the form of a declaration of the person to whom they pertain. An employer has the right to request that the personal data of persons referred to above should be documented. An employer may request that other personal data are additionally submitted if the obligation to submit them arises from separate provisions.

The Act of 18 July 2002 on provision of services via electronic means uses the definition of “personal data” in the wording defined by the Act on personal data
protection while requiring that own provisions be applied to processing of these data. The first difference that has the form of a restriction in relation to the rules provided for in the Act on personal data protection consists in subjecting (by the Act on provision of services via electronic means) the personal data to protection irrespective of whether the processing is carried out within a data collection. The purpose of processing personal data of a service user by a service provider is to establish, formulate, modify or terminate legal relationship with a service user whereas the personal data that may be process by a service provider include: surname and names of the service user, identification PESEL number or – in case when this number was not awarded – passport number, personal ID number or number of another document confirming the identity, registered residence address for permanent stay, mailing address if it differs from the residence address for permanent stay, the data used to verify the digital signature of a service user, electronic address of a service user.

Processing of other personal data by the service provider is admissible, provided that they are necessary to carry out legal operations other than the indicated ones or to perform a contract. In such a case, a service provider is obliged to mark such data as necessary for implementation of the mentioned goals. Furthermore, it is possible for a service provider to process personal data that are necessary to provide services, provided that a service user grants consent to that. The information obligation for a service provider within the meaning of the Act on provision of services via electronic means consists in assuring a constant and easy access for a service user by means of an ICT system used by the service provider to the information about:

- the possibility of using the service provided via electronic means anonymously or by means of a pseudonym (a service provider can make a list of personal data of a service user with a pseudonym chosen by them),
- the technical means provided by a service provider to prevent unauthorised persons from obtaining or modifying the personal data sent via electronic means,
- the entity to which data processing, the scope thereof and planned deadline for submission if a service provider has entered into an agreement with that entity on the assignment of processing of such data such as surname and names of the service user, PESEL identification number or – in case when this number was not awarded – passport number, personal ID number or number of another document confirming the identity, address, but also the data used to verify the digital signature of a service user.

The Act of 6 September 2001 on access to public information is a legal act that excludes the application of provisions of the Act on personal data protection in reference to specific entities. Pursuant to the Act on access to public information, public authorities and other entities performing public tasks are obliged to provide access to public information. In Article 4(1), the Act presents a list of entities obliged in particular to provide access to public information, including but not limited to: the entities that pursuant to separate regulations represent the State’s Treasury and the entities that represent state legal persons or legal persons of the territorial self-government and the entities that represent other state-owned organisational
units or organisational units of the territorial self-government, entities that represent other persons or organisational units that perform public tasks or administer public assets and legal persons in which the State’s Treasury, territorial self-government or economic or professional self-government units are the dominant entities within the meaning of the regulations on protection of competition and consumers.

With reference to persons holding public offices – in the scope of information connected with the performance of these functions – the restriction of the right to public information due to privacy of a natural person does not apply. In this sense, the provisions of the Act on personal data protection do not form the basis for refusal to provide information about such persons.

The Act of 16 July 2004 – **Telecommunication Law** – governs, *inter alia*, the matter of personal data processing by providers of commonly available ICT services, by stipulating that “the contents or data covered by telecommunication secrecy can be collected, saved, stored, elaborated, modified, deleted or made available solely when these activities, hereinafter referred to as ‘processing’, pertain to the service provided for a user, or they are necessary to deliver it” and by listing a catalogue of personal data for the processing of which a provider of commonly available ICT services is entitled.

The Act of 6 July 2001 on detective services stipulates e.g. that a detective must not assign personal data processing to another entity, which is a restriction to a certain degree of the application of provisions of the Act on personal data protection. With reference to detectives, the application of certain provisions of the Act on personal data protection that pertain in particular to “the information obligation” has also been precluded.