VERSITA

STUDIES IN LOGIC, GRAMMAR AND RHETORIC 32 (45) 2013

DOI: 10.2478/slgr-2013-0008

Alina Miruć
University of Bialystok

LIMITS OF THE PROHIBITION OF USING PERSONAL DATA OF SOCIAL ASSISTANCE BENEFICIARIES

Abstract. The objective of this paper is to present the limits of using personal data of the social assistance beneficiaries. Therefore, it will analyse issues concerning such terms as personal data, the essence of its protection, the essence of the limit in personal data use, acceptability and rules of personal data processing on the grounds of both general and specific legal solutions included in the Act on Social Assistance.

It is important to emphasise that the limits of using personal data of the persons benefitting from social security are determined by means of legal solutions referring to personal data protection. The basic regulation in this question is APDP of 29 August 1997, and specific solutions may be found foremost in Article 100 ASA of 12 March 2004, which implies that in the proceedings on social assistance benefits it is important to pursue primarily the good of social assistance beneficiaries, as well as protection of their personal rights. In particular, the names of social assistance beneficiaries and the type and range of the benefit granted must not be published. On the other hand, to a degree necessary for granting and allotting social assistance benefits, it is allowed to process personal data of applicants for and users of these benefits referring to: ethnic origins, state of health, bad habits, convictions, statements of penalties, as well as other statements issued in judicial or administrative proceedings. The existence of exceptions which allow making beneficiaries' personal data available is justified. Every acceptance of revealing social assistance beneficiaries' personal data is subject to many provisions of universally binding law, due to which beneficiaries may protect their rights and good name.

1. Introduction

In Poland, in accordance with the binding law, granting social assistance benefits should occur in accordance with the principle of extraordinary nature, i.e. the rule of personal data protection of the people using social assistance benefits. Among these values the Civil Code lists, for example: health,

ISBN 978–83–7431–371–1 ISSN 0860-150X

freedom, dignity, name, freedom of conscience, secret of correspondence and provides for their general protection. In the case of their infringement we may demand to repair the harm caused by the infringement, especially/such as an appropriate statement, cash compensation, or a payment of certain amount of money to a specified charity by the person commitinng infringement. (Sierpowska, 2006, pp. 71–72).

In the ustawa z dnia 12 marca 2004 r. o pomocy społecznej – on Social Assistance, hereinafter referred to as ASA (Dz. U. z 2009 Nr 175, poz. 1362) the legislator refers directly to protection of personal rights.[1] It is important to underscore that it is one of the tasks for the Social Assistance Administration, which determines proceedings of social assistance benefits, for the legislator obliged the bodies conducting the proceedings in social assistance cases to protect personal rights of the social assistance beneficiaries as well as to pursue the good of these people. In social security cases this protection is of a particular importance, for benefitting from social assistance may be connected with the sense of shame and an intention to conceal this fact.

The objective of this paper is to present the limits of using personal data of the social assistance beneficiaries. Therefore, it will analyse issues concerning such terms as personal data, the essence of its protection, the essence of the limit in personal data use, acceptability and rules of personal data processing on the grounds of both general and specific legal solutions included in ASA.

2. The term 'personal data' and the essence of its use

The provisions of ASA include a general rule of pursuing the good of social assistance beneficiaries and protecting their personal rights in administrative proceedings in social assistance benefits. It is, however, important to note that the term *personal rights* is broader than *personal data* and includes such values as health, freedom, freedom of conscience, name and secret of correspondence.

According to the solutions in the ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926) – Act on Personal Data Protection – hereinafter referred to as APDP – personal data is recognised as "any information concerning a natural person identified or identifiable". (Barta, Fajgielski, Markiewicz, Retrieved from Lex Sigma on-line). This definition corresponds basically with that of *individual data* in the ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U.

z 2012 Nr 591 j.t.), which recognises it as "*personal data* which can be connected with a particular natural person" (further on it was added that individual data is also the individual data which can be connected with business entity or another legal entity, or else an organisational unit not being a legal entity).

Because the Polish noun *dane* (data) has no singular form, (Szymczak, 1995, p. 337) sometimes a proposal is raised to replace the term *personal data* (dane osobowe – plural) with another term, for instance *nominal information*, for the noun *information* in Polish may be used in both singular and plural forms. (Harla, 2001, p. 38). However, the literature raises an argument that the expression *personal data* accurately conveys the essence of the notion in point and, moreover, it is a precise counterpart of the terms used in Directive 95/46/EC (Official Journal L 281, 23/11/1995 P. 0031 – 0050) in English (*personal data*) and in German (*Personenbezogene Daten*), which also occur in plural only.

The definition of personal data in Article 6 of APDP embraces the following elements (premises): (Barta, Fajgielski, Markiewicz).

1) information,
2) concerning a natural person,
3) identified or identifiable.

The first premise in the definition under analysis concerns information. It is understood as communications (messages, speeches, presentations) expressed and recorded in any way: with graphic signs, symbols, in a computer language, in a photograph, on an audio or a video tape etc.) regardless of the method, range and freedom of making them available as well as regardless of the way of their acquisition.

The literature indicates the need for an interdisciplinary agreement on the term information and proposes a definition in accordance to which information is "a transferable (intangible) property reducing uncertainty." (Szpor, 2008, p. 8). There is also a consent on the broad understanding the semantic field of the term *information* used in the definition of personal data. This term should embrace not only language signs but also other circumstances accompanying language signs, or else, only non-language information. (Drozd, 2007, p. 44).

Part of the information used in social relations quite frequently concerns more than one natural person and is strictly connected with one of the qualities of information, which is understood as "unlimited possibilities of linking." (Drozd, 2008, p. 31). In connection with the aforesaid appears a problem of assigning such information to a concrete natural person. It seems reasonable to argue that in a particular situation certain information

is recognised as personal data of this natural person with whom they are connected to the highest degree, which may be decided through, for example, the purpose of personal data processing.

It is assumed that an email address belongs to the category of personal data only when it includes the information on the first name and the surname of the user or "other information like this". (Barta, Markiewicz, 2002, p. 290). On the other hand, W. Zimny (2002, p. 8) holds another position. In his opinion every email address is included in the term personal data. According to X. Konarski, (2004, p. 165) an email address belongs to the category of personal data if the user's identifier in the address is his first name and surname, or if the entity providing the service of electronic mail boxes collected the user's personal data during signing the agreement on providing the services.

The object of the protection guaranteed by APDP is personal data of living natural persons, which are identifiable, where identifiability should be understood as a possibility of connecting the information with a concrete natural person. This information may refer to any type of relations, both personal and property relations, professional achievements, education and character traits. (Fischer, 2010, p. 56). Too restrictive interpretation could, however, lead to qualifying practically any information as personal data. The information should concern a natural person and communicate something on this person.

Thus, an identifiable person is understood as a person whose identity may be determined directly or indirectly, especially through referring to the identity number or else one or more specific factors defining his/her physical, physiological, mental, economic, cultural and social features. However, the information which requires excessive expenses, time and actions to be established is not considered as information enabling to determine a person's identity. (Bunikowski, 2008, p. 74).

The doctrine includes various conceptions on the categorisation of personal data. Two dominating ones are emphasised. One is the theory of spheres, which divides any human's behaviours and personal data referring to them as intimate, private and public. The other is the theory of mosaic which assumes that individual personal data permeate and complement each other. Juxtaposed, they may reflect different aspects of personal life, including the sphere of privacy and even intimacy. (Fajgielski, 2008, p. 32).

3. The essence of the limit of the prohibition of using personal data

Thus, the notion of personal data is not homogeneous. Article 27 of APDP distinguishes data of special nature, the so-called sensitive data (delicate), as opposite to the so-called ordinary data (common), in order to introduce more intense protection of sensitive data and establish separate rules for the processing. (Drozd, 2007, p. 51). APDP recognises sensitive data as data concerning (Barta, Fajgielski, Markiewicz): racial background, political views, religious or philosophical beliefs (this refers also to atheistic and agnostic positions; this category does not, however, include moral principles), affiliations with a religious denomination, a political party or a trade union (also the fact of not belonging and quitting the organisation), state of health, genetic code, bad habits (including withdrawal treatment or abandoning it, participation in groups and organisations with the aim of combating addictions), sexual life, convictions, decisions on punishment, penalty fines as well as other decisions/sentences issued in judicial or administrative proceedings.[2]

The above enumeration of sensitive data is comprehensive. In some cases some ambiguities may occur if a particular piece of information on a particular person does not reveal, for example, his/her religious or political beliefs, or allow the reader to infer his/her race or ethnic background. A broad category is data on the state of health, and therefore certain doubts arise if some information, as sensitive data, should be subject to intense protection.

The criterion of data division into sensitive and ordinary is constituted by the fact that they concern directly spheres of privacy and even intimacy of a natural person. In the remaining cases (e.g. with ordinary data, neutral data, trivial data) the intrusion into privacy either does not occur at all, or even if it does it is not from the very substance of the data but rather from their juxtaposition or context. This division is important for indicating the limits of the prohibition of using personal data of the people benefitting from public security.

The provision of Article 27 section 1 of APDP introduces a rule of the prohibition of sensitive data processing, regardless of the form of processing (automated or traditional). Decisions allowing to process such data are then exceptional regulations. ASA contains such provisions.

APDP introduces several exceptions, included in a closed catalogue, to the rule that sensitive data processing is prohibited. This operation of the legislator decides on the prohibition of applying extensive interpretation. It is also important to underscore that each of the circumstances justifying sensitive data processing is of autonomous and independent nature. Con-

sequently, for example, in the situation where such processing is carried out on the basis and within the limits of a specific regulation, it cannot be recognised as illegal.

When the commonly binding law allows the processing of sensitive data, we should, while transferring them or making them available, emphasise that we deal with this type of data (either directly, or even through the annotation *confidential*). Such behaviour, we may say, is adequate to the obligation, imposed on the administrator, of particular care in order to protect the interests of the persons whom the data concern. (Drozd, 2008, p. 31).

4. Acceptability and rules of personal data processing

The term *data processing* is broad and embraces any operation on personal data, including collecting, recording, storing, developing, changing, publishing and removing. (Fajgielski, 2008, p. 33). General bases of acceptability of data processing were outlined in Article 23 of APDP, constituting a basis for the legalisation of processing.

A condition allowing for personal data processing is a written consent thereto of the person whose data are to be used. The specificity connected with the particular nature of sensitive data involves the requirement that the consent must be in writing. (Fischer, 2010, p. 62).

The other circumstance legalising the processing of sensitive data is particulary liberal provision of another act of law, e.g. ASA. Therefore, it is exclusively a regulation included in the source of law of the status of statute, with a reservation that this regulation must provide full guarantees of the protection of these data. It is important to note that the assessment if a particular provision (or broader, a particular regulation) meets this condition, may in certain concrete situations be a subject of disputes. (Barta, Fajgielski, Markiewicz).

The third premise allows processing personal data as the result of entering into an agreement in order to implement it. This concerns only the situation of processing the data of the parties of this agreement. There may also occur a necessity for processing data, which is a condition of entering into the agreement on demand of the person whom the data concern. (Fischer, 2010, p. 63).

The fourth premise embraces a situation where data processing is indispensable to perform certain legally determined tasks carried out for the public good. In the literature it is accurately pointed out that this provision

concerns exclusively "non-executive actions of the public administration (in forms proper for private law). Executive actions require, in accordance with the basic principle of public law, a precise authorisation in regulations." (Fischer, 2010, p. 63).

The fifth general premise accepts personal data processing for legally justified ends implemented by data administrators or data recipients, and the processing does not infringe the rights and liberties of the person whom the data concern.

On the basis of the analysis of the APDP provisions and the provisions of Directive 95/46/EC P. Fajgielski (2008, pp. 17–26) distinguished ten general principles of processing and protecting personal data: the principle of reliability and legality of processing; the principle of purposefulness of processing; the principle of data adequacy; the principle of substantial correctness of the data; the principle of time limit of processing; the principle of informing about processing, the principle of respecting the rights of the people whom the data concern; the principle of confidentiality and security of the data; the principle of control of the data processed as well as the principle of using sanctions for the infringement of the norms of data protection.

Processing and protection of personal data are based on the norms determined by law. Among them of particular importance are just general principles referring to the activity of entities processing personal data. The principles of processing and protecting data are the basic rules which constitute the essence of legal protection of personal data. They are of particular importance for applying and interpreting the regulations on personal data protection. For the infringement of the principles of personal data processing the law envisages punishments, which are specifically regulated in Articles 49–54 of APDP.[3]

5. Specific solutions in the Act of 12 March 2004 on Social Assistance

Granting benefits from social assistance is an important public task of the social assistance administration. In view of the binding law the organs of social assistance are obligated to obey the general rules determined by the Constitution of the Republic of Poland, the Code of Administrative Procedures and ASA. (Miruć, 2010, pp. 533–543; Nitecki, 2008, p. 89).

The Act on Social Assistance refers directly to the principle of personal data protection. Foremost this principle is a determinant of conduct in the

case of social assistance benefits. The aforementioned term *personal right* should be attributed with a broad meaning and it should be interpreted in the context of the principles and purposes of social assistance. (Nitecki, 2008, 58). In accordance with Article 100 section 1 of ASA the main principle of conduct in the case of granting benefits is pursuing the good of the people benefitting from social assistance and the protection of their personal data.

Article 100 section 1 of ASA forms specific principles strictly connected with the limits of the prohibition of using the personal data of people receiving benefits from social assistance, including the principle of pursuing the good of the parties of the proceedings, the principle of intense protection of personal rights of the party as well as the principle of prohibition of publishing the data identifying the party and the range of the entitlement granted him/her by social assistance.

Article 100 section 2 of ASA basically determines more precisely the limits which reach the prohibition of using the personal data of the parties receiving benefits. This prohibition does not concern the course of proceedings in the case of benefits as well as the stage in implementing the decision on granting the benefit. (Maciejko, Zaborniak, 2010, p. 385).

The principle of pursuing the good of the party receiving benefits in its structure is close to the code principle of taking into consideration the right interest of the party in administrative proceedings. It embraces every case of the occurrence of the necessity for the good of a person in need who is not able to overcome his/her difficult life situation with his/her own resources, capabilities and rights. Social assistance organs are obligated to take into consideration the good of the party of the proceedings if this party meets the statutory conditions of granting him/her the benefit, and in the case of discretionary benefits, if it fits in the actual, i.e. organisational and financial, capabilities of the commune or the district.

The prohibitions in Article 100 section 1 of ASA concerning publishing personal data are listed as examples after the phrase *in particular*. In particular the protection is provided for names and other data of the persons who were granted the aid. In accordance with the provisions of ASA it is forbidden to publish or reveal the type and the range of the benefit granted, i.e. in practice it is prohibited to hang lists of the beneficiaries' names, publish them in local press or the Internet. This prohibition should be also considered in the context of declining granting a benefit because of the lack of financial resources. (Sierpowska, 2006, p. 383). According to judicature the decline should be supported by evidence and justified in details. In view of the wyrok Naczelnego Sądu Administracyjnego (Supreme Administrative Court – hereinafter referred to as SAC) w Warszawie z dnia 9 grudnia 1999 r.

benefit amounts depend on, among other things, the financial capability of the commune. (I SA 2407/99). However, in the opinion of the Court, the commune organs are not entitled to transfer the information on the beneficiaries and the type and range of the benefit granted. The aforementioned prohibitions should be also interpreted in the light of social workers' responsibilities, including the obligation of pursuing the principles of professional ethics and keeping confidential the information acquired during their professional activities.

The Polish social assistance law also limits the freedom of collecting information on current and potential beneficiaries. The legislator accurately envisaged the possibility of processing some personal data of the beneficiaries of social assistance, for certain data on a person, e.g. concerning his/her health are simply necessary to establish the basis for granting the aid. Thus, the point is the personal data processing for the needs of the entity granting the benefits only, and the processing cannot cause any transfer of information outside.

Personal data, or concrete information on: ethnic origins, state of health, bad habits, convictions, decisions on punishment and other statements issued in administrative and civil proceedings, may be processed only in the scope indispensable to grant the aid. SAC, in its decision of 2 March 2001 argued that a social assistance centre granting benefits determined by the state of health of the person applying for a benefit has the right to collect and process the information on his/her state of health when it has an important influence on the recognition of the life situation of the person applying for the aid. (II SA 401/00).

Personal data processing by the organs exercising the rights and responsibilities determined by the provisions of ASA, in particular in Article 2, 3 and 36, is acceptable when it is indispensable to exercise the right or perform the responsibility resulting from a provision of law (Article 23 section 1 point 2 of APDP). The process of processing the personal data of beneficiaries is carried out exclusively in connection with the proceedings concerning granting social assistance benefits on the basis of ASA.

Data processing means operations on personal data such as: collecting, recording, storing, developing, changing, publishing and removing. The legislator envisaged different degrees of protection depending on whether it concerns ordinary data or sensitive data. Ordinary data is any information allowing to identify a person, which are not listed in the closed catalogue of sensitive data. Sensitive data, on the other hand, are: the data informing on racial or ethnic origins, political, religious or philosophical views, affiliation with a religious denomination, a party and a trade union, state of

health, genetic code, bad habits, sexual life, information on criminal records. (Chrapek, 2010, p. 124).

The premises legalising personal data processing are of great importance. (Chrapek, 2010, pp. 125–127). In view of the binding law, as far as ordinary data processing is concerned, which means any information allowing to identify a person, the conditions of personal data processing include: the person's consent, unless it is about removing the data concerning him/her; it is indispensable for performing legally determined tasks carried out for the public good as well as it is necessary to achieve legally justified ends pursued by data administrators or data recipients and the processing does not infringe the rights and liberties of the person whom the data concern.

In the case of particularly sensitive data, for example: origins, political views or the state of health, the premises legalising personal data processing include: a written permit of the person whom the data concern, unless it is about removing his/her data; a specific provision of another act of law allows to process such data without the consent of the person whom the data concern and provides full guarantees of their protection; processing such data is indispensable to protect vested interests of the person whom the data concern or another person, when the person whom the data concern is not physically or legally capable of expressing consent, until the time of establishing a legal guardian or curator; the processing relates to the data necessary to pursue a legal claim; the processing concern the data which have been published by the person whom the data concern, or else, if data processing is conducted in order to exercise rights and responsibilities resulting from a decision issued in judicial or administrative proceedings.

In reference to ordinary personal data, personal data processing is acceptable when it is indispensable to exercise a right or to perform a responsibility resulting from the provision of law. According to the provisions of APDP, on the other hand, sensitive data processing is acceptable if the specific provision of another act of law allows to process such data without the consent of the person whom the data concern and provides full guarantees of their protection. Such a provision is Article 100 ASA, which introduces an option of processing the data particularly protected to the degree necessary for providing benefits. This regulation enumerates the types of particularly protected data, which may be processed. The data particularly protected may be processed only to the degree necessary to grant and allot social security benefits. The provision of ASA forbids to collect the enumerated data in any case but only if granting or declining of granting the benefit

is, in accordance with ASA, dependent on obtaining certain information, e.g. ethnic origin, the state of health or convictions.

An important issue is also the rules of processing the personal data of social assistance beneficiaries. Here we can undoubtedly list: the principle of legality, the principle of purposefulness, the principle of adequacy, the principle of data correctness and the principle of time limit (according to M. Chrapek).

In view of the general principle significant for the whole system of law, which is the principle of legality, organs of public authorities are obligated to act on the basis of law and within its limits. Thus, processing the data of social security beneficiaries should be carried out in compliance with law, or fulfil foremost the premises of legality of personal data processing indicated in APDP and the special act, i.e. ASA, and these operations should be in compliance with executive regulations related to this matter.

In turn, the principle of purposefulness indicates that personal data processing should occur exclusively for legal purposes. Thus, the person processing personal data cannot conceal the purpose from the person whom the data concern. The aim should also not be outlined in too general terms.

The principle of relevancy or necessity indicates that the personal data administrator may process them only to the degree which is indispensable for the purpose of data collecting. The content of ASA this principle expressed literally in Article 100 para 2, in reference to particularly sensitive data, i.e. referring to ethnic origins, state of health, bad habits, decisions on penalties. Undoubtedly this principle should also refer to ordinary data. (II SA/Wa917/2005). Ordinary data should also be processed to the degree necessary to reach the goals of social assistance.

Another rule referred to as the principle of data correctness means that the personal data administrator commits himself to secure the correctness of personal data, which means their accordance with the truth, validity and completeness. The beneficiary of social assistance should update and verify personal data.

The principle of time limit also plays an important role. In view thereof personal data are stored in the file by the administrator not longer than it is necessary to achieve the aim. It is strictly connected with the principle of purposefulness. One group of data may be erased or sent to the archive on the basis of the binding law.

Every person whose personal data are processed has certain rights that protect his/her privacy. Among them are: the right to exhaustive information on processing the date which concern him/her; the right to complete, update or correct the data as well as to demand to stop their processing

or their erasure; the right to demand in writing to stop data processing because of the extraordinary situation of the person whom the personal data concern, as well as the right to protest against data processing if the administrator intends to process the data for marketing purposes or if his/her personal data are transferred to another data administrator. (Chrapek, 2010, pp. 131–132).

It is also worth mentioning that in accordance with ASA, granting a benefit does not depend on expressing a consent to personal data processing.

Every beneficiary should also be allowed the refusal of making personal data available by the organ of public administration. The refusal is written but not in a form of administrative or any other decision. Thus the refusal of making personal data available is neither an operation nor an act of public administration referring to granting, stating or recognising a right or responsibility resulting from provisions of law.

The currently binding law indicates exceptions which allow possibilities of making the social assistance beneficiaries' personal data available.

It is APDP that indicates making personal data in family if community interviews available by social assistance centres for the family if community interview includes sensitive data. In order to make it available to another entity as a whole there must exist a specific provision of law which allows such an operation. Social assistance centres are entitled in view of law to demand access to personal data from another organ, if they are of importance for deciding on granting a benefit or its amount (e.g. from a court of law, a public prosecutor or the police on the beneficiary's service in prison). In this question also a probation officer has the right to demand from the police and other state organs and institutions, local government organs, associations and community organisations within the range of their activities, as well as from natural persons assistance in performing their official duties, which involve making information available to the particular supervised. These data, however, must be indispensable in order to correctly perform official duties. An exception is a family and community interview. The guardianship court may order the probation officer to conduct a community interview as well as to turn for information to a proper organisational unit of social assistance in order to establish important data. It is also important to note that managers of social security centres may transfer to managers of canteens, for example in schools, lists of the names of the people who were granted aid in the form of a meal, which constitute both the basis of financial settlements between the centre and the canteen, as well as serve to identify the persons

attending a meal. This list is not, however, an infringement of personal data protection.

6. Concluding remarks

Summing up these reflections, it is important to emphasise that the limits of using personal data of the persons benefitting from social assistance are determined by means of legal solutions referring to personal data protection. The basic regulation in this question is APDP of 29 August 1997, and specific solutions may be found foremost in Article 100 ASA, which implies that in the proceedings on social assistance benefits it is important to pursue foremost the good of social assistance beneficiaries, as well as protection of their personal rights. In particular the names of social assistance beneficiaries and the type and range of the benefit granted must not be published. On the other hand, to a degree necessary for granting and allotting social assistance benefits it is allowed to process personal data of applicants and users of these benefits referring to: ethnic origins, state of health, bad habits, convictions, statements of penalties, as well as other statements issued in judicial or administrative proceedings.

The existence of exceptions which allow making beneficiaries' personal data available is justified. As you can see, every acceptance of revealing social assistance beneficiaries' personal data is subject to many provisions of universally binding law, due to which beneficiaries may protect their rights and good name.

N O T E S

[1] Particularly Articles 100, 2, 3 and 36.

[2] The amendment to APDP of 25 August 2001 included into the catalogue of sensitive data the information concerning convictions, decisions/sentences on punishment and penalty tickets, as well as other decisions/sentences issued in judicial or administrative proceedings, the processing of which had previously been the subject of regulation of Article 28 section 1 of APDP, which in the previous wording required only a statutory basis for processing this type of data.

[3] Article 49 1. A person, who processes personal data in a data filing system where such processing is forbidden or where he/she is not authorised to carry out such processing, shall be liable to a fine, a partial restriction of freedom or a prison sentence of up to two years. 2. Where the offence mentioned in point 1 of this article relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade-union membership, health records, genetic code, addictions or sexual life, the person who processes the data shall be liable to a fine, a partial restriction of freedom or a prison sentence of up to three years.

Article 50 A person who, being the controller of a data filing system, stores personal data incompatibly with the intended purpose for which the system has been created, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

Article 51 1. A person who, being the controller of a data filing system or being obliged to protect the personal data, discloses them or provides access to unauthorised persons, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to two years. 2. In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

Article 52 A person who, being the controller of a data filing system violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised takeover, damage or destruction, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

Article 53 A person who, regardless of the obligation, fails to notify the data filing system for registration, shall be liable to a fine, the penalty of restriction of liberty or deprivation of liberty up to one year.

Article 54 A person who, being the controller, fails to inform the data subject of its rights or to provide him/her with the information which would enable that person to benefit from the provisions of this Act, shall be liable to a fine, partial restriction of freedom or prison sentence of up to one year.

REFERENCES

(Ed.) Szymczak, M. (1995). *Słownik języka polskiego*, Volume 1. Warszawa: PWN, 337.

Barta, J., Fajgielski, P., R. Markiewicz. *Ochrona danych osobowych. Komentarz*, *Edition* V. Retrieved from Lex Sigma on-line.

Barta, J., Markiewicz, R. (2002). *Ochrona danych osobowych. Komentarz.* Kraków: Zakamycze, 290.

Bunikowski, D. (2008). Podstawy aksjologiczne prawa ochrony danych osobowych. In G. Goździkiewicz & M. Szabłowska (Eds.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów* (p. 74).Toruń: TNOiK "Dom Organizatora".

Chrapek, M. (2010). *Pomoc społeczna w pytaniach i odpowiedziach: wybrane zagadnienia.* Warszawa: Infor Expert, 124.

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 (Official Journal L 281, 23/11/1995 P. 0031 – 0050).

Drozd, A. (2007). *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy.* Warszawa: LexisNexis, 44.

Drozd, A. (2008). Pojęcie danych osobowych. In P. Fajgielski (Ed.) *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, (p. 31). Lublin: Wydawnictwo KUL.

Drozd, A. (2008). *Zabezpieczenie danych osobowych.* Wrocław: Presscom, 31.

Fajgielski, P. (2008). *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne.* Lublin: Wydawnictwo KUL, 32.

Fajgielski, P. (2008). Zasady ogólne przetwarzania i ochrony danych osobowych. In G. Goździewicz & M. Szabłowska (Eds.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów* (pp. 17–26). Toruń: TNOiK "Dom Organizatora".

Fischer, B. (2010). *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich.* Warszawa: Wolters Kluwer, 56.

Harla, A. (2001). Termin "dane osobowe" – uwagi de lege lata i de lege ferenda na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. *Palestra*, 1, 38.

Konarski, X. (2004). *Komentarz do ustawy o świadczeniu usług drogą elektroniczna.* Warszawa: Difin, 165.

Maciejko, W., Zaborniak, P. (2010). *Ustawa o pomocy społecznej. Komentarz.* Warszawa: LexisNexis, 385.

Miruć, A. (2010). Zasady ogólne Kodeksu postępowania administracyjnego w procedurze przyznawania pomocy społecznej. In J. Niczyporuk (Ed.), *Kodyfikacja postępowania administracyjnego na 50-lecie k.p.a.* (pp. 533–543). Lublin: Wydawnictwo Wyższej Szkoły Przedsiębiorczości i Administracji.

Nitecki, S. (2008). *Prawo do pomocy społecznej w polskim systemie prawnym.* Warszawa: Wolters Kluwer, 89.

Sierpowska, I. (2006). *Prawo pomocy społecznej.* Kraków: Kantor Wydawniczy Zakamycze, 71–72.

Szpor, G. (2008). Pojęcie informacji a zakres danych osobowych. In P. Fajgielski (Ed.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, (p. 8). Lublin: Wydawnictwo KUL.

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2012 Nr 591 j.t.)

Ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2009 Nr 175, poz. 1362).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 Nr 101, poz. 926).

Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 2 marca 2001 r., II SA 401/00, *Wokanda* 2001, 9, p. 33.

Wyrok Naczelnego Sądu Administracyjnego w Warszawie, z dnia 9 grudnia 1999 r., I SA 2407/99, Lex 48595.

Zimny, W. (2002). Czy adresy e-mailowe są danymi osobowymi? *Biuletyn Ochrona Informacji*, *2*, 8.