THE RIGHT TO BE FORGOTTEN AS AN ELEMENT OF THE PERSONAL DATA PROTECTION SYSTEM IN THE ORGANISATION

Monika ODLANICKA-POCZOBUTT[1*], Aleksandra SZYSZKA-SCHUPPIK[2]

[1] Silesian University of Technology, Faculty of Organisation and Management, Department of Management and Logistics, monika.odlanicka-poczobutt@polsl.pl, ORCID: 0000-0001-7834-1188
[2] Silesian University of Technology, Faculty of Organisation and Management, Department of Management and Logistics, aleksandra.szyszka-schuppik@polsl.pl, ORCID: 0000-0002-6535-4059
* Correspondence author

Introduction/background: The protection of personal data, as the protection of information on natural persons by entities which hold it, is currently a topic of considerable interest. Proper protection of personal data is closely related to the way the organisation is managed. Lack of management awareness of the dangers of inappropriate procedures in this respect can lead to abuse and even crime, e.g. identity theft. In the light of doubts as to whether to rely on existing solutions or build a system from scratch, there are many research problems in this area.
Aim of the paper: The cognitive goal of this article is to analyse the basics of building a system of personal data protection in the scope of creating new internal regulations and to indicate the role of the Data Protection Officer, while the utilitarian goal is to analyse the case of a request to erase the processed data.
Materials and methods: A selected organisation was studied, where a process map with a detailed description of actions was drawn up on the basis of participant observation and direct interviews.
Results and conclusions: The conclusions indicate that the Data Protection Officer may perform the function of a person responsible for the system. However, their activities must be supported by information obtained from within the organisation. Therefore, it is important to involve the highest management in the development of the personal data protection system. The foundations for creating a procedure to handle the request for erasure of personal data were also indicated.

Keywords: personal data security, GDPR, personal data processing, Data Protection Officer, right to be forgotten, erasure of personal data.

1. Introduction

Personal data protection is currently a popular topic that generates more and more interest. What is more, social awareness of data protection law is growing, also with regard to data entrusted or shared with other entities. Recently, a closer look has been taken at various

institutions, checking whether the technical and organisational solutions applied by them are sufficient for the data to be secure (https://uodo.gov.pl/pl/138/1189).

This was facilitated by the entry into force of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – hereinafter referred to as the GDPR. The purpose of implementing this Regulation was to establish a uniform level of personal data protection in all Member States of the European Union.

Personal data, according to the definition in Art. 4 of the GDPR, is all information about an identified or identifiable natural person. Pieces of individual information, which when combined may lead to the identification of a person, are also personal data. This is indicated by Opinion 4/2007 on the concept of personal data adopted by the Article 29 Data Protection Working Party on June 20th, 2007. Such data can be e.g. name and surname, or the personal identification number (PESEL) of an individual. In its opinion, the Working Party also points to biometric data, including not only fingerprint, retinal pattern, facial structure, but also the venous system "or even some deeply rooted skills or other behavioral characteristics (such as handwritten signature, keystrokes, special walk or speech pattern etc.)". (Opinion of the Article 29 Working Party 01248/07/PL WP136 No 4/2007, p. 8).

Personal data, which has been stripped of its identifying elements or encrypted or pseudonymised, but which may lead to reidentification of a natural person, remains personal data within the scope of the GDPR (Article 4(1) and (5) of the GDPR). Pseudonymised data cannot be attributed to a specific person without the use of additional information (Elliot, O'Hara, Raab, O'Keefe, Mackey, Dibben & McCullagh, 2018). Proper pseudonymisation is subject to the condition that such additional information is stored separately and is subject to technical and organisational measures that make it impossible to attribute it to an identified or identifiable natural person. The literature review revealed that university institutions across Europe organised courses, both formal and informal, to prepare staff for the new incoming GDPR legislation. Academic institutions feel the obligation to treat personal data with care and respect, following the provisions of GDPR. (How the General Data Protection Regulation changes…, 2019).

Personal data anonymised in a way that data subjects cannot be identified at all or can no longer be identified shall not be deemed personal data. For data to be genuinely anonymous, the anonymization must be irreversible (Article 29 Working Party Opinion 0829/14/PL WP216 No. 05/2014, p. 6).

Pseudonymisation is thus a process which aims at reducing the risk related to personal data processing; however, this is still personal data, so provisions of Articles 15-20 of the GDPR are applicable (Mourby et al., 2018, p. 223).

The protection of personal data is the protection of information concerning natural persons by entities that manage them, i.e. controllers. The protection applies both to individual information constituting personal data and to entire compilations and sets of data. This obligation results directly from Art. 47 of the Constitution of the Republic of Poland: "Everyone shall have the right to legal protection of their private and family life, their honor and good reputation, and to make decisions about their personal life" and Article 51(1) of the Constitution: "No one may be obliged, except on the basis of legislation, to disclose information concerning themselves." (The Constitution of the Republic of Poland, Art. 47-51).

The protection of personal data is understood as the protection of data against loss, leakage, or unauthorised access, i.e. preventing the data to be processed by persons not authorised to do so (https://poradnikprzedsiebiorcy.pl).

The GDPR ensures personal data protection, regardless of the technology used to process the data. Thus, it is "neutral with respect to technology" and is applicable both to automated and manual processing, if the data is or is to be included in a set of data. That is what recital 15 of the GDPR directly points to. Furthermore, it is irrelevant how the data is stored, whether in an IT system, a video surveillance system or a paper-based system – in all of which cases personal data is subject to the protection requirements of the GDPR (https://ec.europa.eu/info/law).

Nowadays, teleinformatic systems support operations in almost all areas of life. They are used in every institution, both in small organisations and small enterprises. They are key determinants of the level of development of the state and, above all, of the quality of operation of its organisational and administrative structures. The intensification of criminal activities aimed at theft and illegal use of information on IT networks is steadily increasing, as is the number of available services and the volume of gathered information resources (Kępa, 2012, p. 60.).

Each organisation has a certain specificity determined by the principles of personal data protection. Uncritical copying of elements from other organisations' policies is strongly discouraged. However, it is possible to use in an organisation those elements justified by organisation and management theory (Grzelak, 2015, p. 56.).

Proper protection of personal data is closely related to the way the organisation is managed. Lack of awareness of the organisation's management about the risks and potential losses resulting from the lack of procedures regulating data protection may contribute to abuse and even criminal offenses in the information flow (Bajorek, 2016, pp. 40-50). After more than a year of the GDPR being in force, there are still doubts about the construction of a proper system of personal data protection, which is to ensure that the data will not only be processed correctly, but above all, will be properly protected against unauthorised access.

Many controllers, despite compliance with the requirements of the no longer applicable Act of 1997 on personal data protection (Journal of Laws of 2016, item 922, as amended), still cannot cope with issues arising from compliance with the GDPR. They cannot identify all

of their obligations and have problems with establishing rules, instructions or procedures that will guarantee compliance with formal and legal requirements included in the GDPR, often unconsciously exposing organisations to the risk of a penalty imposed by the Personal Data Protection Office (UODO), which, during the audit, could indicate irregularities and impose financial penalties in the amount of up to EUR 20 million (art. 83 GDPR).

In the light of doubts as to whether it will be correct practice to base the system on existing requirements and implemented solutions, or whether it should be built from scratch, there are many research problems in this area. The cognitive goal of the article is to analyse the basics of building a system of personal data protection in the scope of creating new internal regulations, while the utilitarian goal is to analyse the case of a request to erase the processed data. A selected organisation was studied, where a process map with a detailed description of actions was drawn up on the basis of participant observation and direct interviews.

2. The role and tasks of the Data Protection Officer

Before May 25th, 2018, most data controllers did not pay sufficient attention to personal data processing. On the basis of the authors' experience – some of them did not implement any solutions in their organisations, even those required by law, and some were limited to meet only minimum requirements, including among others the development of safety policy and instruction of IT system management, the appointment of an information safety administrator or, where an information safety administrator was not appointed, the registration of personal data sets.

After the GDPR came into force, controllers first had to consider whether they would appoint a Data Protection Officer (DPO) in the place of an information safety administrator. Some controllers did not have this dilemma, as the obligation to appoint a DPO results directly from Art. 37 of the GDPR, which states that "Data controller and processor shall appoint DPO always when:

a) the processing is carried out by a public authority or entity, with the exception of courts, as regards the exercise of justice or
b) the main activity of the controller or processor consists of processing operations, which, by their nature, scope or purpose, require regular and systematic large-scale monitoring of data subjects or
c) the main activity of the controller or the processor is large-scale processing of special categories of personal data".

The obligation to appoint a DPO applies to public entities, defined in such way regardless of the nature of their activity and the scale of personal data processing, as well as the volume, type or deployment of organisational solutions (Jabłoński et al., 2018, p. 84).

In other situations, appointment of a DPO is not mandatory, but, according to the guidelines of the Article 29 Data Protection Working Party, it is recommended within "good practice" (Guidelines for Data Protection Officers (DPO) WP 243 rev. 01, p. 7).

The responsibilities of the DPO are specified in Article 39 of the GDPR and they include:

a) information tasks consisting of informing the controller, the processor and persons who process data about their obligations dictated by the GDPR,
b) monitoring compliance with GDPR and other regulations governing the processing of personal data, e.g. the Personal Data Protection Act of 2018,
c) carrying out activities aimed at raising the awareness of the controller, the processor and the employees or other persons processing the data,
d) training personnel,
e) conducting audits that verify the correctness of personal data processing – the quantity, frequency and scope of audits is established by the DPO themselves; however, it is recommended to discuss the audit schedule with the controller,
f) co-operation with the Personal Data Protection Office,
g) make recommendations on request for the data protection impact assessment and monitor its implementation in accordance with Article 35,
h) acting as a contact point for the supervisory authority on processing issues, including prior consultation. This obligation also results from Art. 38(4) of the GDPR, which points out that "Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation" (Jabłoński et al., 2018, pp. 103-104).

Article 38 of the GDPR clearly states that "the data protection officer is involved, properly and in a timely manner, in all issues, which relate to the protection of personal data". At the same time, section 2 orders the controller and the processor to support the activities of the Officer in the fulfilment of their tasks. Unfortunately, it often turns out that, without additional support, the DPO is not able to manage data protection in an organisation on their own; their activities require the establishment of a team of people who will be responsible, together with the DPO, for the management of personal data. The DPO must be supported by information from other people, such as managers of individual departments such as human resources, marketing, finance and accounting and, of course, the IT department.

The biggest problem faced by the Officers is to obtain reliable and comprehensive information on data processing, including not only the manner of data protection, but also the scope, purpose and time of data processing. The DPO often receives information post factum, after commencement of data processing, which in practice prevents them from properly fulfilling their obligations.

The consequence of the lack of knowledge of the DPO may be, for example, a breach of the principles set out in Article 25 of the GDPR, i.e. "Data protection by design and by default" – the principle called *privacy by design* and *privacy by default*. These are the principles which

state that the controller has to take data protection and privacy issues into account at every stage of data processing, starting from obtaining the data. It is therefore reasonable to involve the DPO in processes within the organisation that are directly related to the protection of personal data. The essence of the role of the data protection officer in the organisation is not the subject of research in this article, therefore it was not given much attention. The focus was on the right to be forgotten.

3. Basis for building a personal data protection system

Due to the complexity of the processes related to the appropriate protection of personal data, it seems that in each company it will be justified to establish a team responsible for the implementation, construction and maintenance of a personal data protection system.

The first stage of team's work should be to determine which personal data the organisation processes. The Processing Activity Register maintained in accordance with Article 30 of the GDPR is a document helpful in establishing the factual situation. This document was not required before the entry into force of the GDPR, but the controller was obliged to keep the Register of Personal Data Sets. These two documents have the same purpose – determining what data is actually processed by the controller. The Processing Activity Register is kept in order to ensure compliance with the GDPR and enable the Supervisory Body, i.e. DPO, to monitor the correctness of personal data processing (recital 82 of the GDPR). In practice, it is a very important element of the personal data protection system – this document allows the systemisation of activities carried out within the framework of data processing (Guidelines and explanations on the obligation to register processing activities and categories of activities stipulated in Art. 30(1) and (2) of the GDPR, GIODO Information materials, p. 5). It is a kind of inventory of activities, manners of data processing, and the safeguards used.

The register should contain such information as:

- the precise identification of the controller – including the contact details of the controller,
- details of DPO – if one was appointed,
- purpose of data processing,
- description of data subject categories and personal data categories,
- categories of recipients,
- and other elements, pursuant to Art. 30 of the GDPR.

The register can contain additional elements, e.g. legal basis for processing, source of data, used software and information on the need to carry out a data protection impact assessment (DPIA).

The team should then carry out a risk analysis based on the information collected in the course of its work. This obligation results from recital 83, which obliges the controller to "assess the risk" and implement measures that minimise it. The GDPR does not stipulate these measures; however, it states that these measures "should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected" (recital 83).

An important material that should be used in the work of the team are recorded incidents, i.e. adverse events that could have an impact on the integrity, availability and confidentiality of the processed data, e.g. by making them available to unauthorised persons. Therefore, such an important element of the system of personal data protection is the recording of incidents and drawing conclusions from them for the future, which is a legal requirement mandated by Article 35(5) of the GDPR. In the case of Officers who outsource their services, the input to risk analysis may also be incidents with other controllers, where this person also performs the functions of DPO.

As in other situations, for risk analysis, the GDPR gives controllers the freedom to choose their own risk assessment method. Controllers can use recital 75 of the GDPR for their risk analysis, which lists examples of risks, e.g.:

- discrimination and/or identity theft
- financial loss,
- damage to the reputation,
- loss of confidentiality of personal data,
- unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage,
- deprivation of rights and freedoms or of the possibility to exercise control over one's personal data and other.

Only a detailed risk analysis of personal data processing can provide the basis for the development of a dedicated personal data protection system and the definition of appropriate technical and organisational measures to secure the processed data.

4. Procedure of exercising the right to be forgotten

The right to erasure, also known as "the right to be forgotten" is one of the rights of data subjects. Data subjects also have the right to information, the right of access, the right of rectification, the right to limit data processing, the right to object to data processing, the right to data portability and the right not to be subject to decisions based solely on automated processing.

The right to erasure applies only in selected cases. One of them is achieving the purpose for which the data were collected (Art. 17(1)(a) of the GDPR). This obligation of the controller is closely linked to the rules of data processing stipulated in Art. 5 of the GDPR – the personal data shall be "collected for specified, explicit and legitimate purposes and not processed further in a manner that is incompatible with those purposes". Furthermore, such data may be stored no longer than is necessary for the purposes for which they were collected and processed (Art. 5(1)(e) of the GDPR). As a rule, it is the controllers themselves who, without waiting for the request of the data subject, should observe the principle of limiting the processing of personal data (Litwiński et al., 2017, p. 402).

Another, yet not the last case, may be the withdrawal of consent. Art. 17(1)(b) explicitly stipulates the data subject's right to withdraw their consent, if the processing took place based on Art. 6(1)(a) (ordinary data) or Art. 9(2)(a) (special categories of data, e.g. concerning health, sexuality, religious beliefs, etc.).

This article will discuss the procedure to be followed when a request for erasure of data is sent to the controller in relation to the withdrawal of consent to the processing.

When there is a request to erase processed data, organisations often do not know what to do. If the data subject:

- claims that the data is no longer necessary for the purposes for which it was collected or processed otherwise,
- withdraws the consent which is a basis for processing and there is no other legal basis for the processing,
- objects to the processing of their data,
- claims that personal data were processed unlawfully,
- claims that the data has to be erased in order to fulfil the controller's legal obligation,
- claims that personal data was collected in connection with the provision of information society services

then the data subject (pursuant to Art. 17(1) of the GDPR) can request the controller to erase the data.

Due to the lack of an agreed procedure in the event of a request to erase data, the authors decided to carry out the research in the form of participant observation and direct interview. The information obtained in this way will constitute the basis for the development of detailed procedures, dedicated to a specific company, for handling a request for data erasure, and the creation of a graphical process map.

Participant observation consists primarily in the researcher entering a given social environment and observing a specific group from the inside as one of its members. At the same time, it is a direct observation, whereby the researchers themselves collect data, as well as hidden and uncontrolled observation (Cybulska, 2013, p. 21).

The use of the research method based on participant observation is justified by the fact that the co-author of this article processed the request to be forgotten in one of the organisations. Thus, the below procedure was developed based on a specific event which concerned a particular organisation.

The interview, as one of research techniques, helped in collecting and organising data. In the present situation, these research techniques seem to be the most appropriate to the specificity of the request to be forgotten. Lack of experience in handling this type of request has led the authors of the article to use a non-directive unstructured interview, conducted on the basis of a general plan of issues. The questions asked were open and induced the respondent to provide multi-layered, longer statements (Przybyłowska, 1978, p. 63).

The applied methods are used for analyses in industry, but also in services, administration and project management.

Based on the collected information, a process map for data erasure in the organisation was developed. The manner of implementing the data erasure process, including also particular activities performed by specific persons, were presented in a graphic form. Developed in such way, the process map presents its structure and the sequence of actions that are performed during the process (Keller, 1999, pp. 62-64).

On the basis of the information collected, it was established that a company dealing with the sale of equipment and providing services in the field of maintenance and repair of such equipment received, by electronic means, a request to erase data.

The Company, which was the addressee of the request, despite the absence of a legal obligation, appointed a Data Protection Officer. The Officer provides their services under a civil contract, not as an employee of the Company. After receiving an e-mail from the data subject with a request to erase data, the DPO was informed about the fact of receiving such request.

The request has to be processed, regardless of its form of submission (e.g. by e-mail, phone, mail). In justified cases, e.g. when submitting the request by phone, an organisation has the right to additionally verify the identity of the person submitting the request (e.g. contacting the person by e-mail to an e-mail address stored in the database). The condition for starting the erasure procedure is the correct verification of the identity of the applicant. In this particular case, there was no need to additionally verify the person's identity – the received e-mail clearly defined who made the request.

The controller should, without undue delay – and in any event within one month of receipt of the request – provide the data subject with information on the actions taken in relation to the request. If necessary, this period may be extended further by two months, due to the complexity of the request or the number of requests. Within one month of receiving the request, the controller informs the data subject of such an extension, stating the reasons for the delay.

Where the data subject has transmitted their request electronically, the information is, as far as possible, also transmitted electronically, unless the data subject requests otherwise.

After receiving a request to erase data, the controller should verify whether one of the prerequisites entitling the data subject to request erasure specified in Article 17(1) of the GDPR is met.

After receiving the request, the following should be verified:

- in which computer system the data was processed,
- if the data has been archived,
- if the data was processed in a traditional, paper manner,
- to whom the data was transmitted,
- if processors also have access to the data,
- which of the employees in the organisation is responsible for managing the applicant's data.

The organisation has the right to reject a request to erase data when processing is necessary:

- to exercise the right to freedom of expression and information (e.g. in the case of the press, media, electronic forums or comments on websites),
- to comply with a legal obligation requiring processing under EU law or under the law of the Member State, to which the controller is subject, or to carry out a task performed in the public interest or to exercise official authority vested in the controller,
- for reasons of public interest in the field of public health, pursuant to Art. 9(2)(h) and (i), as well as Art. 9(3) of the GDPR,
- for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1) of the GDPR, if the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing,
- for the establishment, exercise or defense of claims.

A simplified procedure chart for dealing with requests for erasure is presented on figure 1.

The diagram presented by the authors of the study is of a general nature. On its basis, each organisation creates its own instructions that are tailored to its specific conditions.

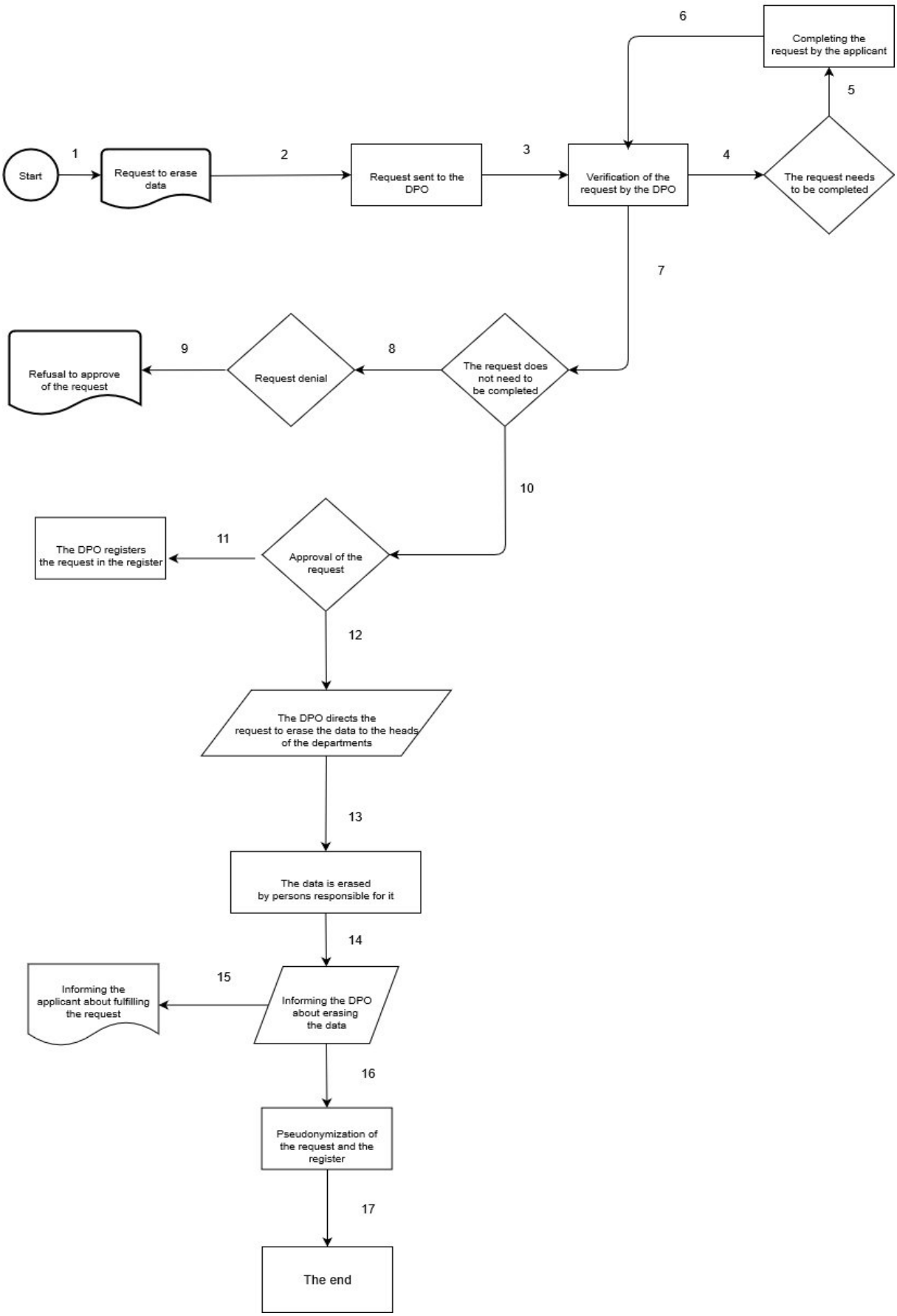

Figure 1. A map of processes implemented in the analysed company, divided into identified activities. Source: own study.

Situation description:

The company received an e-mail with a request to erase data [1]. The applicant requested data erasure by sending an e-mail from a business address consisting of the name, surname and domain of the company. The e-mail was sent to a dedicated e-mail address gdpr@abc.pl. Due to the fact that the company uses the services of a DPO specialist outside the company, the request email was sent directly to the DPO [2]. The request was verified by the DPO – it was complete and clearly stated the person it concerned [7]. Therefore, there were no grounds for requesting data to be completed [step 5 and 6]. The next step was to analyse whether the person's request was justified. The application, which was received by the company, concerned the withdrawal of consent to the processing of personal data with the simultaneous request to erase it. The DPO registered the request in an electronic register kept by them [11]. Then, the DPO, in consultation with the representative of the department responsible for processing the data of that particular person, verified whether any of the prerequisites set out in Article 17(3) of the GDPR are met. This verification has shown that the request of the person is justified and that the data should be erased. Therefore, the DPO ordered the head of the department by e-mail to erase the data [12]. The data was erased according to the DPO's instruction [13] and the DPO [14] and the applicant [15] were informed of this fact. The next step was to pseudonymise the register and the request received by the DPO – the contact details in the e-mail were pseudonymised and the e-mail was deleted. The DPO stores only the pseudonymised copy of the e-mail (request) and register [16]. The case is closed [17].

Data erasure includes the deletion of all the applicant's data processed by the organisation (e.g. financial and accounting IT system, e-mail elements, security copies, CMR, CMS, office software files, paper documents etc.). In the example presented above, the request concerned erasure of data of a person subscribed to a newsletter. The data has been deleted from the current, valid database; it has not been deleted from the backups (Politou, Michota, Alepis, Pocs & Patsakis, 2018). Deleting data from backups raises a lot of questions – not only because of an absent or limited technical possibility to carry out such an operation, but also because of the correct reproduction of the altered backup (erasure of data of a particular person). The performed pseudonymisation of the request will allow for the possible repeated erasure of the data if there is a need to restore the data from the backup, which seems reasonable in order to guarantee the rights of the applicant while ensuring the integrity and availability of the database (Gawroński et al., 2018 pp. 252-254).

However, the position of the Ministry of Digital Affairs is different, with clear instructions to erase data from back-up copies as well: "Personal data must also be erased from all backups and logs. If erasing single records from backup threatens to infringe the integrity of other collected data, the controller can manually restore the copies to the main database, and then erase single records from them and create backups of the database without this record, although it is a quite time-consuming process" (Ministry of Digital Affairs, p. 6).

Once the controller has decided to erase the data, no further processing can be permitted.

5. Summary

The cognitive purpose of the article was to analyse the basics of building a system of personal data protection with respect to creating new internal regulations. Due to the complexity of the issue, only some elements were analysed. The article focuses only on the basics of building a system of personal data protection. Only issues related to the functioning of DPO in the organisation and problems with identification of a team of persons responsible for its implementation were discussed.

The utilitarian goal was to analyse a case of a request to erase processed data. Based on the developed process map with a detailed description of actions, the basis for the preparation of the procedure has been laid down, which may become an essential element of the data protection system. The procedure outlined above once again indicates that the protection of personal data requires the involvement of more than just the DPO. Of course, the DPO's duty is to coordinate the whole process, but it also requires the involvement of other people, such as those responsible for processing the data and implementing the physical erasure of the data in the IT system. The DPO also keeps required records and is responsible for correspondence with an applicant. The presented scheme is one of the possible options of the procedure of executing a request for data erasure. The solutions proposed in this article may provide guidelines for other organisations, but should be modified depending on the size and specificity of the organisation and whether the DPO is an employee of the organisation or provides services on an outsourcing basis.

The authors' experience clearly shows that the controllers' approach of shifting the full responsibility for the system to the DPO is inappropriate and may lead to the risk that the organisation might fail to comply with the obligations resulting from the GDPR. DPO may be the person responsible for the system, but their activities must be supported by information from within the organisation. It often happens, especially in the case of outsourcing DPO functions, that the DPO is not informed about the conducted processes and discovers them by accident. That is why it is so important to involve the senior management in building a system of personal data protection, at least at the beginning, and to involve the DPO in the process of managing the organisation. At a later stage, the position of the DPO in the organisation may prove so strong that they will be able to fulfill their duties independently, with only little internal support. Until then, however, the DPO needs to be supported by an internal team.

Further research in this area will therefore include other elements that should form the basis for building a well-functioning system of personal data protection in an organisation.

References

1. Bajorek, J. (2016). Ochrona i bezpieczeństwo danych osobowych w organizacji. *De Securitate, No. 1(2)*.
2. Constitution of the Republic of Poland of 2 April 1997 (JoL of 1997, No. 78, item 483).
3. Cybulska, D. (2013). *Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej – Obronność, No. 2(6).*
4. Elliot, M., O'Hara, K., Raab, C., O'Keefe, C.M., Mackey, E., Dibben, C., McCullagh, K. (2018). Functional anonymisation: Personal data and the data environment. *Computer Law & Security Review, 34(2),* 204-221. doi:10.1016/j.clsr.2018.02.001.
5. Grzelak A. (2015). *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości*, Warszawa: Oficyna Wydawnicza SGH.
6. Guidelines of the Article 29 Working Party 16/EN WP 243 rev.01 Guidelines on Data Protection Officers („DPO"), adapter on 13 December 2016, last amended and adapted on 5 April 2007.
7. *How the General Data Protection Regulation changes the rules for scientific research.* Panel for the Future of Science and Technology. EPRS European Parliamentary Research Service Scientific Foresight Unit (STOA). PE 634.447 – July 2019. ISBN: 978-92-846-5045-3 doi: 10.2861/17421.
8. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected_pl, 25.08.2019.
9. https://poradnikprzedsiebiorcy.pl/-na-czym-polega-ochrona-danych-osobowych, 25.08.2019.
10. https://uodo.gov.pl/pl/138/1189, 17.05.2020.
11. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf, 15.06.2020.
12. Jabłoński, M., Sakowska-Baryła, M., Wygoda, K. (2018). *Czy jesteśmy gotowi na RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*. Wrocław: Uniwersytet Wrocławski.
13. Keller, P.J., Jacka, M. (1999). Process mapping. *Internal auditor, No. 5.*
14. Kępa, L. (2012). *Dane osobowe w firmie. Praktyczny poradnik przedsiębiorcy.* Warszawa: Difin.
15. Kunda, K., Gawroński, M. (2018). Prawa jednostki. In: M. Gawroński (ed.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO ze wzorami*. Warszawa: Wydawnictwo Wolters Kluwer.
16. Litwiński, P., Barta, P., Kawecki, M. (2017). *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, komentarz.* Warszawa: C.H. Beck.

17. Ministerstwo Cyfryzacji, *RODO – informator,* https://www.gov.pl/web/cyfryzacja/rodo-informator, 20.08.2019.
18. Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S.E., Bell, J., Smith, H., Aidinlis, S., Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review, 34*.
19. Opinion of the Article 29 Working Party 01248/07/PL WP136 No. 4/2007 on the definitione of personal data, adapter on 20 June 2007.
20. Opinion of the Article 29 Working Party 0829/14/PL WP216 No. 05/2014 on technology for anonymization, adapted on 10 April 2014.
21. Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review, 34(6)*, 1247-1257. doi:10.1016/j.clsr.2018.08.006.
22. Przybyłowska, I. (1978). *Wywiad swobodny ze standaryzowaną listą poszukiwanych informacji i możliwości jego zastosowania w badaniach socjologicznych.*
23. Regulation (EU) 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 Directive 95/46/EC.
24. Regulation of 29 August 1997 on personal data protection (JoL 2016, item 922, as amended).
25. *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO.* Materiały informacyjne GIODO.