LEGAL BASES FOR THE GDPR IMPLEMENTATION IN MARKETING

Lenka Hanáková

Abstract

Business entities carrying out marketing activities are among those which are fundamentally affected by the protection of personal data provided by the GDPR Regulation. Personal data is part of a personal identity and a very valuable and strategically important commodity these days. The importance of this legislation therefore is that it unifies the protection of personal data of individuals across the EU, it is directly applicable legislation. Business entities work with personal data from existing or potential customer when implementing marketing activities. The successful application of GDPR to marketing of business entities assumes a very good knowledge of this legislation and the ability to apply it correctly to the various processes and procedures that the business entity or marketing agency implements in the marketing field. All personal data controllers and processors are required to introduce technical, organizational and procedural measures in accordance with the GDPR. No matter how big the institution or business entity is. This subject is very broad. With a view to the limitation of this contribution, the main aim is therefore to present and discuss only some selected aspects of this issue (knowing that a number of other sub-themes will be worked in the future), to highlight a number of questions that arise in relation to this theme, to outline the potential direction and methods of the future research.

Keywords: *Marketing, GDPR, personal data, controller, pseudonymization, anonymization*

1 INTRODUCTION

The European Data Protection Regulation (hereafter referred to as GDPR or GDPR Regulation) became applicable as of 25 May, 2018, in all member states for any company that stores or processes personal information about EU citizens within EU states. Voss (2014) notes that despite the fact that the European Union had legislation in the area of data protection, yet there were reasons for change. The choice of a regulation as the EU legislative instrument was made, because regulations will be in force in the same form in all of the member states of the European Union. He also points to the support of uniformity of law in the EU, which contrasts with the differing ways of implementation of Directive from 1995 in the various EU member states. Similarly, Tankard (2016) states that "since it is a regulation, not a directive, compliance is mandatory, without the need for each member state to ratify it into its own legislation". In addition, he points to an important fact, namely that "the GDPR expands the scope of data protection so that it applies to anyone or any organization that collects and processes information related to EU citizens, no matter where they are based or where the data is stored".

The collection and storage of personal data in the European Union is governed by the principles of minimal disclosure (data minimization principle) and of the duration of the minimum storage of personal data (conservation principle). These general principles were stipulated in the Data Protection Directive in a broad way and applied to any processing of personal data (ENISA, 2012). Although Directive 95/46/ES was repealed as a result of the adoption of the GDPR, according to Recital 9 of the GDPR, its objectives and principles remain sound. However, there is still a widespread public feeling that there are risks in relation to the protection of personal data of individuals, particularly with regard to activities carried out online.

The GDPR Regulation constitutes a set of rules for the protection of personal data. These legal rules apply to any body that collects and processes the personal data of Europeans. This means that these rules also bind those companies and institutions outside the EU that operate in the European market. Put simply, any entity that works with the personal data of its customer, clients or suppliers and that monitors and analyses user behavior on the web when using apps or smart technologies must follow GDPR Regulation. To think that the GDPR Regulation represents a revolutionary change in privacy is inaccurate. In the Czech Republic, there was an act No. 101/2000 Coll., on the protection of personal data, which regulated personal data processing obligations. By this act Directive 95/46/EC was implemented into the Czech legal order. Although the obligation to implement this Directive had to be met by all EU Member States, there was a differing level of personal data protection between EU member states; it was due to differences in the implementation and application of this Directive. So what is the role of the GDPR Regulation? It is directly applicable in all EU member states, not necessary to implement it. The reason is to ensure a uniform level of protection for individuals across the EU (Recital 13 of GDPR Regulation). The GDPR refines personal data processing obligations, introduces some new institutes and rights, and also toughens the penalties stemming from breaches of them. EU states were required to adopt an implementing law to specify more than 50 points that the GDPR places under the national jurisdiction of individual member states. The Czech Republic fulfilled this obligation with an annual delay. Act No. 110/2019 Coll., on the processing of personal data, came into effect 24. 4. 2019. He replaced the existing national law (Act No. 101/2000 Coll.).

This paper deals with selected aspects of GDPR in conjunction with marketing. The issue of GDPR is a very wide-ranging issue that takes a lot of time not only to gain knowledge of the content of this legislation, but especially to understand the processes. The author of this contribution proceeds from the assumption, that the level of burden imposed by the GDPR Regulation and the financial, organizational and staffing impacts will be perceived differently by business entities. This depends on the size of the business entity and its focus. Recital 13 of the GDPR Regulation explicitly mentions that "To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes derogation for organizations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/ES".

Business entities, and in particular marketing agencies, are among those subjects whose marketing activities are heavily impacted by the GDPR Regulation. If these entities have performed responsibly the obligations laid down by national legislation before the GDPR took effect, then the GDPR does not necessarily represent a revolutionary change for them. Potůček (2017) states that the effects will be different in a small trading company that has a corporate website, but does not collect any e-mails to send newsletters, just only uses the contact form or cookies. Different impacts can be expected for a business entity that operates an e-shop, has multiple communication channels, sends out newsletters regularly, and uses remarketing or targeted advertising.

The main objective of this article, taking into account the broad scope of the whole issue of GDPR in conjunction with marketing, is to address some of the core and, for the purposes of this contribution, selected problems that business entities must take into account and may face.

The structure of the article is as follows. First, the article will address some of the basic legal concepts of the GDPR Regulation, such as personal data and why it is important to distinguish

when a personal data is involved and when it is not. The difference between controller and processor will be explained as this distinction can cause problems and some uncertainty in practice, however this distinction is crucial for business entities – it is linked to the GDPR´s determination of obligations and especially the responsibilities involved. Another area of concern will be anonymization and pseudonymization, their benefits and potential risks to business entities in relation to the processing of personal data of individuals will be discussed. Secondly, possible targets of interest, potential direction and methods of the future research under PhD study will be identified.

This contribution is an initial step in the search for topics to be given particular attention within the planned focus group and subsequent qualitative eventually quantitative research.

2 BASIC LEGAL CONCEPTS OF GDPR REGULATION

2.1 The importance of a subject´s position in the processing of personal data

Veberová (2017) emphasizes, first and foremost, the need to understand the concept of personal data correctly and to distinguish correctly who is in the position of controller and who is in the position of processor. She considers these three things essential and primary, because it enables marketing activity managers to implement the next steps needed to comply with the GDPR Regulation.

Business entities undertake marketing activities to reach both potential and existing clients and to offer them their services or goods and convince them of the uniqueness of their offer. One way in which business entity can implement it, is through digital (on line) marketing. This may be implemented by the business entity itself as a body of rights through its employees, or the business entity can use the services of the marketing agency, then a contract must be concluded. In the first case, the business entity is in a position to both a controller and a processer of personal data. In the latter case, it is essential that there is a clear clarification of roles contractually between the business entity and the marketing agency. The GDPR Regulation in Article 4 (7) defines the term "controller" as follows: „Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data ". Paragraph 8 of the same provision contains the definition of "processor": „Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller ". Finally, it must be taken from how the GDPR Regulation defines "processing", i.e. what all activities are covered by this legal concept. The answer is found in paragraph 2: „Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

The processor of personal data, according to the GDPR, is therefore an entity (person, authority, business entity) that processes personal data on behalf of the personal data controller. It could be, for example, an accounting company, a payroll processing company or a customer data processing marketing company. A written personal data processing contract between the processor and the controller is necessary. However, it should be stressed that the controller has still a responsibility for processing personal data. Simply put, the controller is responsible for his processors and this responsibility cannot be transferred to another entity. This is also why the controller should be very cautious when selecting a processor and why he should select only such an entity that provides sufficient guarantees for the safe processing of personal data. The

importance of the written contract is reflected, inter alia, in the fact that it defines the activities and operations that the processor may carry out, in other words, which he has been instructed to carry out by the controller. The controller is the one with the main responsibility for processing personal data. However, even the processor has obligations, e.g. he is required to properly safeguard the processing of personal data and to comply with adequate organizational and technical measures to prevent personal data being compromised. In addition, the processor has another very important obligation. If he finds out, that a controller is in breach of the obligations laid down by GDPR, he must bring that fact to the controller´s attention while stopping processing personal data. If he fails to do so, the processor shall be liable for the damage caused to the personal data subjects together with the controller.

The GDPR Regulation brought a new legal concept into the Czech legal order – joint controllers. However, this legal term has existed in European law for many years. This term has already been regulated by Directive 95/46/ES, but Czech legislators did not use the option of extending the definition of a "controller" to include more than one entity when implementing that directive into national law. According to the article 26 of GDPR applies as follows: "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects".

Considering the GDPR Regulation, it is therefore necessary to assess correctly situations where more than one entity is involved in the processing of personal data. The definition character of joint controllers within the meaning of Article 26 (2) of GDPR is a joint determination of the purposes and means of processing. However, the GDPR Regulation does not specify in more detail what can be included in the concept of "joint determination". In this context, Nemčeková (2019) states that answers to the interpretative and application ambiguities could be brought by the latest EU Court of Justice (SDEU) case law to the concept of "controller" enshrined in the Article 2 (d) of Directive 95/45, which is defined in it as a "natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purpose and means of processing personal data". The interpretation of this concept is particularly relevant from the point of view of the direct application of the relevant GDPR provisions both at European and national level. Nemčeková (2019) cites two SDEU decisions as an example in this context, namely decisions C-210/16 and C-25/17. The term "controller" is to be interpreted broadly to ensure effective protection of the data subject and their right to privacy, according to the court. She notes that when applying this interpretation of the SDEU to an article 26 of GDPR, it can be concluded that the "joint determination" of purpose and means is to be interpreted extensively. She cites paragraph 43 of the C-210/16 judgment, which states that "it cannot necessarily be inferred from the existence of joint liability that individual operators should bear the same proportion of responsibility. On the contrary, those operators may be involved at different stages of that processing and to varying degrees, so that the degree of responsibility of each of them must be assessed in the light of all the relevant circumstances of the present case". However, as Nemčeková points out, the court did not specify what may be the relevant circumstances from the point of view of the court´s or supervisory authorities´ decision. That this is an interesting and important issue from the point of view of the recipients of the legislation, shows the fact, that the issue of a broad interpretation of the term "joint controllers" and the subsequent responsibilities was addressed by EU Advocate General Michal

Bobek (Opinion of the Advocate General, 2018). In this opinion, the Advocate General points to the practical problem of a broad interpretation of the SDEU, according to which there is no need for each of the controllers to have access to personal data. Such a controller is then responsible for processing, but he cannot effectively provide access to personal data to any data subject. Although that opinion concerns the interpretation of Directive 95/46, the Advocate General points out that the interpretation will also have an impact on the application of Article 26 of GDPR, in particular paragraph 3 – where that provision governs solidary liability of joint controllers and essentially rules out the conclusion that controllers need not have the same liability. He emphasizes the interpretation of the term "processing", which focuses on processing stages, respectively acts or sets of personal data operations. He is of the opinion that the administration should be assessed in relation to specific processing operations. In relation to the responsibilities of joint controllers, he notes in point 101 of the opinion that "As regard a particular processing act, the (joint) controller is responsible for such an act or set of acts for which he shares or co-determines the purposes and means. On the other hand, such a person cannot be held liable for the preceding stages or the subsequent stages of the entire processing chain, in respect of which he could not determine the purpose or means of processing".

With regard to the above, it is clear that determining the status of the entity is absolutely essential. The reason is simple, the entity may not only be in a position of controller, or in the position of processor, but under the GDPR Regulation there is even a "joint controllers". As Nemčeková (2019) points out, the concept of Article 26 of GDPR is based on the assumption that individual entities will be aware of being joint controllers and, based on this knowledge, they will define tasks and responsibilities between themselves. At the same time, however, she points to the practice when the entities have difficulty evaluating the position they are in, even in relation to the processing they carry out themselves. Therefore, determining the reciprocal position they are in when involving other entities in relation to the specific processing of personal data is even more challenging. A common question for obligors is whether one of them is the processor of the other, i.e. the person who processes personal data for the controller (according to his instructions). However, the relationship between the different entities involved in the processing can be diverse, such as the controller – controller relationship, the controller – processor relationship, the relationship of the joint controllers, or the relationship of the controller and the person in charge of processing in the controller´s business, typically the employee.

The correct determination of who is in what particular position (controller, processor, and joint controller) when processing the personal data of individuals is extremely important. Indeed, there is a threat of a penalty (administrative fines under the GDPR are very high – see Article 83 (4), (5), (6) of the GDPR Regulation) and liability for damage caused by processing that infringes the GDPR. This is not just about responsibility in public law, but also in private law. If a business entity in a position of controller or processor demonstrates that he is in no way liable for the event that led to the harm, he is absolved of liability for the harm. The existence of this mitigating ground for absolving liability laid down by the GDPR is absolutely essential for business entities. It means certainty for them to be able to demonstrate that all their activities relating to the personal data of individuals that they carry out in connection with the marketing activities are in line with the GDPR. On the other hand, however, this places considerable responsibility on the business entity in determining and securing all obligations and elaborating all procedure to comply with the requirements of the GDPR. Clarifying the roles in relation to the processing of personal data is crucial in determining the subsequent liability where a breach of a particular legal obligation under the GDPR is found.

2.2 Personal data, anonymization, pseudonymization

Esayas (2015) stresses that understanding the concept of "personal data" is at the center of discussions about the protection of personal data. At the same time, he adds, this is so because the "processing" of "personal data" is the main criteria for the applicability of data privacy rules.

Nulíček et al. (2017) states that the personal data is not only the identifier itself as a birth number or name and surname, but any information about the person associated with that identifier (e.g. a complete record in the personnel system that relates to a particular employee). Similarly, in the case of a business entity, it may be a complete record in a database relating to a particular customer. However, Nulíček et al. stresses that even if we remove all direct identifiers from the record as birth number or name and surname, the specific record may not stop containing personal data if the relevant data can be assigned to a particular individual indirectly. With regard to the possibility of indirect identification, according to Recital 26 of GDPR – into account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. However, the question is how to determine whether the use of means to identify a natural person can be reasonably assumed. Again according to Recital 26 of GDPR – all objective factors should be taken into account, such as the cost and the amount of time that identification will require, taking into consideration the available technology at the time of the processing and technological developments. Nulíček et al. (2017) points to the fact, that the controller should focus on the specific means by which an individual can be retrospectively identified from anonymized data, and also taking into account how costly this retrospective identification is, whether it requires extensive know-how and what is the likelihood that it will occur. It would certainly be much easier for managers of marketing activities if there was a clear and precise definition of the term "personal data". Unfortunately, the legislation is somewhat ambiguous in this sense, as it regards as a "personal data" any information that may lead to the identification of the person.

As Esayas (2015) appropriately complements, identifiability implies that identification has not happened yet but is possible, for example, by combining the information being processed with other information. So it means that the mere possibility of associating certain information with particular individual is sufficient. This wording places a great responsibility precisely on marketing activity managers, who must be able to evaluate when it will be a personal data and when it will not. This decision is subsequently tied to the obligations laid down by the GDPR Regulation. However, what is personal data in case of one individual, because it makes it clearly identified, may not yet be personal data for another natural person. A crucial and decisive factor is whether it is possible to identify a specific person from the data associated with the information. From this point of view, the name of a person itself, or possibly an email in conjunction with a name, will not be a personal data unless it is possible to identify a particular person. A personal data may be just one, provided that it enables a particular individual to be identified in itself. But it will often be more data that only together will allow a specific person to be identified. It doesn´t matter if the controller has this data in one database or in multiple separate databases or lists. While the definition of personal data is relative broad, it must be taken into account that the application of the GDPR Regulation only occurs when it is processed.

Only natural persons have the right to personal data protection under GDPR Regulation. Therefore, all legal persons, public authorities and other institutions are excluded from protection. However, their employees are affected by that protection. Based on the above, marketing activity managers must always take into account the existence of GDPR Regulation

when using these data to contact a natural person, or if any of the personal data are published online, e.g. in the context of a content marketing.

Personal data collected by the controller, whether alone or through a marketing agency, for a particular purpose may be deliberately and specifically anonymized or pseudonymized. The question is whether these processes, i.e. anonymization and pseudonymization relating to the personal data of individuals, are subject to the GDPR regime and what this means for marketing activity managers as a result.

Oswald (2014) has already discussed the importance of anonymization of personal data as a method of minimizing privacy risks and increasing trust. She considers anonymization to be important because it enables secondary use of personal data while minimizing the privacy risk to individuals.

Ohm (2009) says that the anonymization plays a central role in a modern data handling, it forms the core of standard procedures for storing or disclosing personal information. Ohm points out that data controllers anonymize to protect the privacy of data subjects when storing or disclosing data. For various reasons, they may want to disclose the data to another entity, citing the big banks as an example. These may want to share some data with their marketing departments, but only after anonymizing to protect customers´ privacy. However, Ohm also points to a potential problem related to possible re-identification. It is based on the fact that by anonymizing data, a data controller gives notice of his intent to protect the privacy of his data subjects, who may rely on this notice when consenting to provide him their data. He draws attention to the fact that re-identification can happen completely in the shadows. The question then is how in practice do detect an act of re-identification. In this context, he outlines a possible eventual example concerning Amazon.com. Indeed, it is really a fictional example, when Amazon.com anonymizes its customer purchase database and hands it over to a marketing company. The marketing company will promise not to re-identify people in Amazon´s database, but it knows that if it did, it could significantly increase profits. The question remains, if the marketing company breaks its promise and re-identifies, how Amazon or anyone else will ever know. So, according to him, a marketing company can make re-identification in secret and revenue gains may not be detectable for the vendor. Ohm admits that this problem could appear insurmountable, but he also cites possible solutions, such as a bun on re-identification by lawmakers with tougher sanctions and better enforcement or lawmakers can give citizens a private right of action against those who re-identify.

Esayas (2015) states that the term anonymization includes a number of techniques that aim at reducing the identifiability of individuals, and at the same time pseudonymization can be considered as one technique of anonymization. However, he distinguishes between these two terms, especially because of the different legal significance attached to different anonymization techniques under data privacy rules.

Nulíček et al. (2017) refers to the original Directive 95/46/ES, which contained a similar provision concerning the identification of a natural person as the GDPR, in particular its closer interpretation by the Court of Justice of the European Union in the Breyer case. As he points out, it follows from that decision that the possibility of identifying a particular person must be seen objectively, and if there is more than a hypothetical possibility that another person will make identification, the relevant data must be regarded as personal data. Thus, the specific conclusion of that decision was that the dynamic IP address collected by the website operator was a personal data item.

ICO (2012) says, that understanding anonymization means understanding what personal data is and to protect privacy it is better to use or disclose anonymized data than personal data. At the same time, it adds, that effective anonymization depends on understanding what constitutes

personal data. Information or a combination of information, that does not relate to an individual or does not identify an individual, is not personal data.

Nulíčet et al. (2017) argues that in practice, personal data will also be data that the controller adjusts so that they do not contain any more direct identifiers (e.g. by hashing technique) and then the controller passes them on to a third party for processing. The reason for that is the fact that the controller is able to make retroactive identification of data subjects based on the original data, if the original data had not been deleted. In that case, it will be pseudonymized data that is data protected by a security measure reducing the risk associated with the processing. However – these data are still subject to the GDPR regime. At the same time, he points to the ability of the controller to remove completely certain data from GDPR mode. In this context he speaks about anonymization, within which the data are adjusted in such a way that they cannot be assigned to a particular natural person, taking into account any means that can reasonably be assumed to be used by the controller or another person for the direct or indirect identification of the natural person.

Oswald (2014), referring to UK´s Information Commissioner Office (2012) and its advice, stresses that determining whether personal data has been effectively anonymized involves an assessment of risk in order to ensure that the risk is "remote".

Anonymization consists in the removal of information that may lead to the identification of a particular person. In this process, personal data is removed from a document or database. This process, which is irreversible, makes it impossible to assign data in a document or database to specific individuals. This deletion must be done in such a way that no one in a given document or database can find and assign personal data back to a particular natural person. The result of anonymization is therefore a document, database or other media file, however the information contained therein is not attributable to specific persons. This procedure is very often used precisely in marketing in bulk data processing for statistical or evaluation purposes. It is essential for marketing activity managers that this procedure is not subject to GDPR Regulation. Anonymization may be accomplished by, for example, blacking out or blurring an anonymized part of a document or image. How ICO (2012) says anonymization helps organizations to comply with their data protection obligations whilst enabling them to make information available to the public.

There are undisputed positives of anonymization that business entities may feel in relation to the realization of marketing activities. The fact that anonymized data is exempt from the scope of the GDPR Regulation may provide sufficient reason for marketing activity managers to use anonymization in relation to customer personal data. Of course, this is not always possible, especially not in the case of direct marketing, where it is targeted at a particular individual. Nulíček et al. (2017), however, points out, that anonymization is not in practice a matter of a single operation. In this context, he refers to the opinion of WP 29 No. 5/2014 of 10. 4. 2014 on anonymization techniques. According to this opinion, full anonymization can only be achieved by combining multiple methods such as aggregation, permutation or "adding noise". Only by combining more such measures it can be achieved that it is not possible to separate an individual from the dataset, it is not possible to link different records relating to one person and it is not possible to infer information relating to one person from the dataset. In order to declare that personal data are anonymized, these three criteria mentioned must be met.

It should be stressed that pseudonymized personal data is not anonymized data. The consequence is that they are still subject to the GDPR Regulation. The essence of pseudonymization of personal data is the process of hiding the identity of a natural person. It means replacing the identification data of persons (e.g. names and surnames) with some insignificant identifier – a code (e.g. a number). The aim of this procedure is to protect data sets

with personal data so that this data cannot be paired with specific people. Only a person who has the necessary files, which are deliberately kept separately, can correctly assign sensitive data to specific individuals. It is therefore a reversible process, i.e. that it is possible to reconstruct the original file, but it is necessary to have both parts of it to do so. Marketing activity managers always collect personal data with some purpose. The aim may be, for example, to identify target group´s preferences for subsequent adaptation of marketing activities. Pseudonymization is therefore mainly used for the protection of personal data. It makes it impossible to assign a particular person to specific data, which contributes to protection against wanted or unwanted abuse.

The GDPR Regulation in Article 4 (5) defines the term "pseudonymization" as follows: "Pseudonymization means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

Mourby et al. (2018) addresses the question whether the GDPR is expanding the scope of personal data by introducing the term "pseudonymization". He argues that if all data that was "pseudonymized" in the conventional sense (e.g. through coding) should be considered personal data, it would have serious implications for research. Even when he is referring in particular to research relating to data that is collected and stored by public authorities, this can be extended, in the opinion of the author of this contribution, to any research. In this case, marketing research conducted by business entities to target well their marketing activities. Mourby et al. (2018) argues that the definition of pseudonymization does not expand the category of personal data. This definition within the GDPR is not intended to determine whether data is personal data, as all data falling within this definition is personal data. However, he points to Recital point 26 of the GDPR and the requirement contained therein of a reasonable assumption of the use of means to identification of a natural person. He sees this as a test of whether the data is personal. Mourby is of the view that this leaves open the possibility that data that has been pseudonymized in the conventional sense could be anonymized. He also admits that there may be circumstances where data that has undergone pseudonymization within one organization could be anonymous to a third party. The definition of pseudonymization is not to be used, according to his conclusions, to determination whether the data are personal data according to GDPR, as it is indeed clear that the data to which pseudonymization applies are and remain personal data. Instead, point 26 of Recital of GDPR should be used to determine whether the data is personal. The question is therefore whether there are any means that can reasonably be used to identify individuals.

Tsalakis et al. (2016) highlights in the context of pseudonymization that "The additional information needs to be kept separately by the data controller, who must take all appropriate technical and organizational measures to ensure non-attribution". He also points to the fact that "Although recital 28 acknowledges that pseudonymization can reduce risks of personal data breaches, under recital 26 pseudonymized data should still be considered as personal data as they include information relating to identifiable natural persons". He therefore concludes that pseudonymized data are not exempt from GDPR and in order for any dataset to be considered pseudonymized within the meaning of GDPR it shall not be possible to attribute information to identifiable individuals.

ICO (2012) notes that the definition of "personal data" can be difficult to apply in practice, this is especially because, that the term of "identify" and therefore "anonymize" is not straightforward because individuals can be identified in a number of different ways. Firstly, it

may be a direct identification, where someone is explicitly identifiable from a single data source, as for example a list including full names, secondly it may be an indirect identification, where two or more data sources need to be combined for identification to carry out. The problem is that there may be other data somewhere with which a third party will be able to realize re-identification. Apparently, therefore, ICO (2012) says, that it may actually be difficult to determine whether the data has been anonymized or is still personal data.

3 RESEARCH GAP AND OUTLINE OF THE RESEARCH

It is clear from the literary research of selected problem areas relating to the subject that these are topics that are not only important and essential in the field of personal data processing, but also not always quite clear. Thus, they are linked to a number of other follow-up issues that, however, marketing activity managers have to cope with in practice.

It should be stressed that this contribution is only a small illustration of the sub-topics that relate to the author´s main theme, namely – what are the changes in the approach of business entities to marketing after GDPR Regulation took effect. Since the author of this contribution is at the very beginning of the PhD study and research work, the contribution is deliberately focused on the legal bases for the implementation of GDPR in marketing. However, it should be added that, considering the limitation of the range of this contribution, it is not possible to address all the sub-topics that come into account. Nevertheless, the author will certainly address them in other future research work.

With respect to the literary research related, at the moment and for the purposes of this contribution, indeed, really only to a few selected sub-topics, it is evident the existence of a research gap. The research intention therefore aims to fill this gap. The author´s research intention is to analyze and evaluate how business entities (small, medium and large) perceive these sub-themes in practice when implementing marketing activities, how they deal with them in practice, and what implication it has for them, whether in the financial, organizational or staffing fields.

The content of this contribution may lead to the following research questions. 1) Which key marketing activities were affected by the GDPR Regulation? A number of other partial research sub-questions will be answered as part of this research question. For example, whether business entities use anonymization and pseudonymization processes when processing personal data in connection with marketing activities. If so, what real problems they face. Whether they use these personal data processing processes to a greater extent after the GDPR has taken effect. In which marketing activities do business entities use anonymization and pseudonymization processes? Whether business entities have trouble clearly to identify, when implementing their marketing activities, what is a personal data item and what is not. If another entity is used to process personal data, or more than one entity is involved in certain processing of personal data – whether they perceive it easy to determine each other´s roles and positions in processing and if not, how do they deal with it? The first research question leads logically to the second and third research question, namely: 2) what impact (financial, staffing, organizational, etc.) had a GDPR Regulation on management of marketing activities? 3) Is there a difference in the impact of GDPR on the management of marketing activities in small, medium and large business entities, if so, in what areas? The hypotheses will be formulated on the basis of literary research and implemented focus group. They will be confirmed or rebutted on the basic of the implementation of qualitative, or quantitative, research.

The intended procedure of the work and methods in carrying out the research are shown graphically below (Fig. 1).

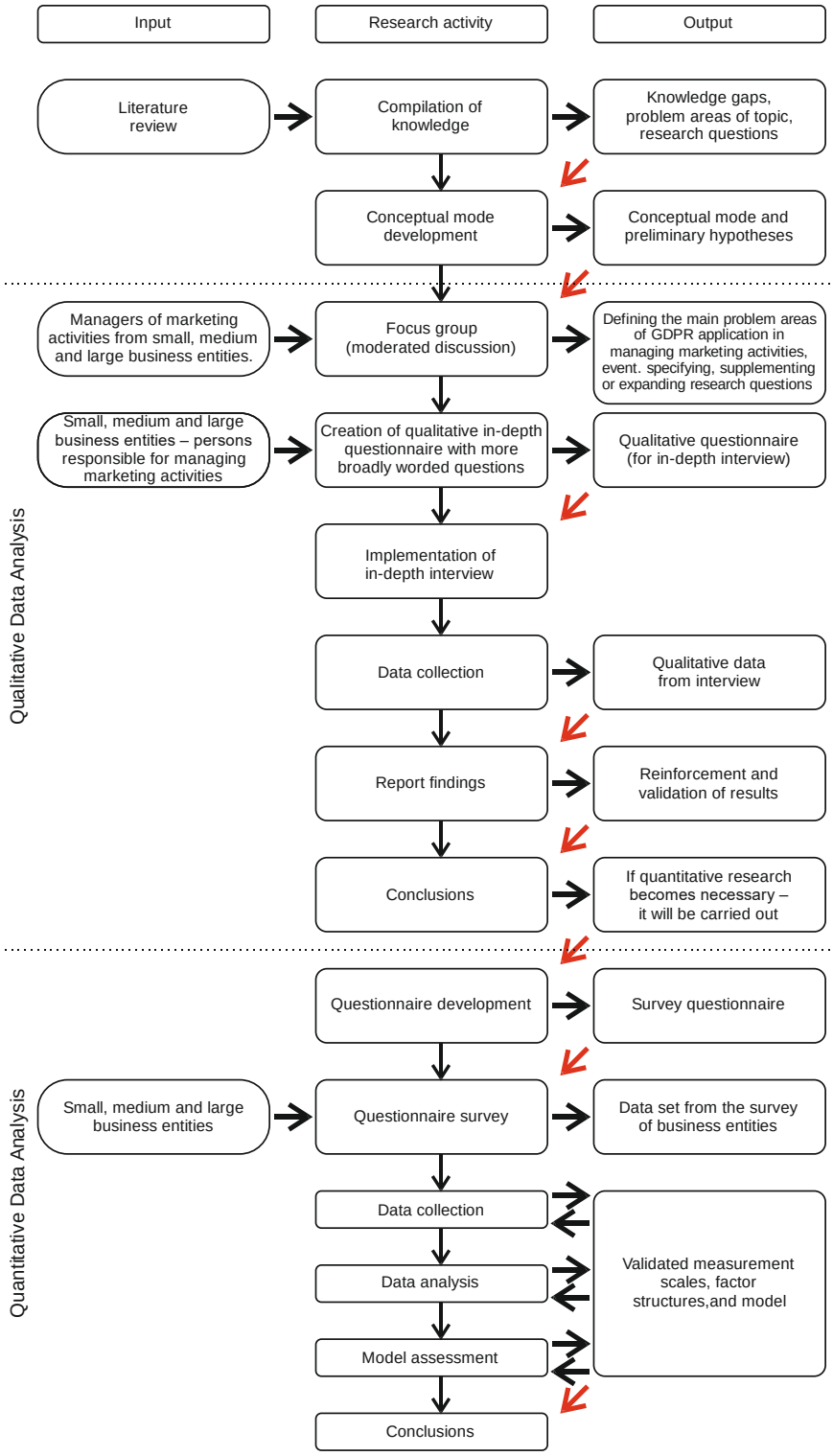

Fig. 1 – Procedure of the work and methods. Source: own research

4 CONCLUSION

Personal data is undoubtedly an important and integral part of an individual´s personal identity. However, they represent a very valuable and strategically important commodity for a number of entities. The GDPR regulation seeks to balance these two, largely conflicting interests. The protection of personal data is gaining a new dimension. Business entities need personal information for their marketing activities to target on a specific entity. Individuals very often

provided their personal data without thinking, for example when shopping online, when registering for various applications and services. The GDPR seeks to respond to the huge technological changes that have occurred since 1995, when the Data Protection Directive 95/46/ES came into force.

Since the author of this contribution is only at the very beginning of the PhD study, the main aim of this paper is to highlight the complexity and breadth of the whole issue – i.e. marketing in conjunction with the GDPR, under which, for this contribution, only some sub-topics have been selected, such as the issue of the definition of personal data, the issue of determining a subject´s position in the context of personal data processing, pseudonymization and anonymization issues.

This contribution presented, taking into account its scope limitation, only some selected aspects of this theme, highlighted some of the questions that arise in relation to this topic, outlined the potential direction and methods of future research.

References

Act No. 110/2019 Coll., on processing personal data. *Collection of laws of the Czech Republic*, 47, 890-911.

Act No. 101/2000 Coll., on the protection of personal data and amending certain laws. *Collection of laws of the Czech Republic*, 32, 1521-1566.

Data Protection Working Party. (2014). *Opinion No. 5/2014 on anonymisation techniques*. Retrieved from https://www.pdpjournals.com/docs/88197.pdf

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

ENISA. (2012). Study on data collection and storage in the EU. In *European Network and Information Security Agency*. Retrieved from https://www.enisa.europa.eu/publications/data-collection

Esayas, S. Y. (2015). The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach. *European Journal of Law and Technology*, 6 (2), 1-23. Retrieved from http://ejlt.org/article/view/378/568

ICO. (2012). *Anonymisation: managing data protection risk code of practice*. Retrieved from https://ico.org.uk/media/1061/anonymisation-code.pdf

Judgment of the Court. (2016). *Case C-582/14*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582

Judgment of the Court. (2018a). *Case C-210/16*. Retrieved from http://curia.europa.eu/juris/celex.jsf?celex=62016CJ0210&lang1=cs&lang2=EN&type=TXT&ancre=

Judgment of the Court. (2018b). *Case C-25/17*. Retrieved from http://curia.europa.eu/juris/celex.jsf?celex=62017CJ0025&lang1=cs&lang2=EN&type=TXT&ancre=

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(2), 222-233. doi: 10.1016/j.clsr.2018.01.002

Nemčeková, I. (2019). K odpovědnosti společných správců. In *Epravo.cz*. Retrieved from https://www.epravo.cz/top/clanky/k-odpovednosti-spolecnych-spravcu-108827.html

Nulíček, M., Kovaříková, K., Tomíšek, J., & Švolík, O. (2017). GDPR v otázkách a odpovědích. In *Bulletin-Advokacie.cz*. Retrieved from http://www.bulletin-advokacie.cz/gdpr-v-otazkach-a-odpovedich?

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation. *UCLA Law Review*, 57(6), 1701-1777. Retrieved from https://www.uclalawreview.org/pdf/57-6-3.pdf

Oswald, M. (2014). Share and share alike? An examination of trust, anonymisation and data sharing with particular reference to an exploratory research project investigating attitudes to sharing personal data with the public sector. *Journal of Law, Technology and Society*, 11(3), 246-272. doi: 10.2966/scrip.110314.245

Opinion of advocate general. (2018). *Case C-40/17*. Retrieved from https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:62017CC0040&from=EN

Potůček, J. (2017). E-maily, cookies, remarketing: Jak vyřešit GDPR na webových stránkách? In *Obsah na dosah.cz*. Retrieved from https://www.obnd.cz/e-maily-cookies-remarketing-jak-vyresit-gdpr-na-webovych-strankach.html

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/ES.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5-8. doi: 10.1016/S1353-4858(16)30056-3

ÚOOÚ. (2018). *GDPR and direct electronic marketing*. Retrieved from https://www.uoou.cz/gdpr-a-primy-elektronicky-marketing/d-30715

ÚOOÚ. (2017). *Controller, Processor*. Retrieved from https://www.uoou.cz/7-spravce-zpracovatel/d-27278

Veberová, L. (2017). GDPR: Již včera bylo pozdě aneb Co je to za novoty. In *Obsah na dosah.cz*. Retrieved from https://www.obnd.cz/gdpr-jiz-vcera-bylo-pozde-aneb-co-je-to-za-novoty.html

Voss, G. W. (2014). Looking at European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later. *Journal of Internet Law*, 17(9), 12-24. Retrieved from https://ssrn.com/abstract=2567624

Contact information

Mgr. Lenka Hanáková
Tomas Bata University in Zlín, Faculty of Management and Economics
Mostní 5139, 76001, Zlín, Czech Republic
E-mail: lhanakova@utb.cz
ORCID: 0000-0002-2242-7588

doi: 10.7441/dokbat.2019.031