DOI: https://doi.org/10.32839/2304-5809/2021-5-93-22
УДК 341.9

Luzan Tetiana
NGO Right to Protection

THE CONCEPT OF PERSONAL DATA: FROM ACADEMIC PERSPECTIVE TO PRACTICAL IMPLICATIONS

Summary. This article is dedicated to the concept of personal data. Although notion of the personal data was introduced to data protection legislation quite a while ago, a number of issues has still remained unresolved. One of such issues is the identifiability, a condition for qualification of certain data as the personal data. This condition ignited an academic controversy resulted in a juxtaposition of the absolute and relative approaches to the concept of personal data and, subsequently, pseudonymised data. Yet, both these approaches are observable in the GDPR. Consequently, application of a moderate approach (in-between the absolute and relative approaches) may be suggested. Application of the moderate approach is a means to balance the protection of personal data against other EU rights and freedoms, such as the conduct of business. Finally, by the way of the moderate approach a legal status of the initial data controller may be distinguished from a subsequent recipient of pseudonymised data.

Keywords: General Data Protection Regulation, personal data, pseudonymised data, identifiability, concept of personal data, absolute approach, relative approach.

Лузан Т.Л.
Благодійна організація «Благодійний фонд «Право на захист»

ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ: ДОКТРИНА ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ

Анотація. Ця стаття присвячена концепції персональних даних. Хоча поняття персональних даних було впроваджено до законодавства про захист даних досить давно, низка питань все ще залишається невирішеною. Одним із таких питань є ідентифікація, умова кваліфікації певних даних як персональних даних. Зазначена умова розпалила академічну дискусію щодо застосування абсолютного чи відносного підходів до концепції персональних даних і, відповідно, псевдонімізованих даних. Згідно з першим підходом під час кваліфікування даних, як персональних даних, слід брати до уваги як контролера даних, так і будь-яку третю особу. Відповідно до другого підходу з метою проведеняя належної кваліфікації даних увагу слід зосередити лише на контролері даних. Проте обидва ці підходи можна знайти в Загальному регламенті про захист даних. Тому, видається за можливе запропонувати застосування поміркованого підходу (між абсолютним та відносним підходами). Така пропозиція може також бути обґрунтована висновками Суду Справедливості ЄС у справі Брейєра. Убачається, що деякі контролюючі органи у сфері захисту персональних даних теж впровадили такий підхід у свою діяльність. Застосування поміркованого підходу є способом гармонізувати захист персональних даних з іншими правами і свободами в ЄС, наприклад, із свободою вести бізнес. Нарешті, застосовуючи поміркований підхід, можливо належним чином відрізнити правовий статус початкового контролера даних від одержувача псевдонімізованих даних. Це означає, що під час визначення правової природи переданих даних слід враховувати й одержувача псевдонімізованих даних (як третю особу). Разом з тим, така оцінка повинна проводитися з урахуванням засобів, які з розумною ймовірністю будуть використані одержувачем для повторної ідентифікації псевдонімізованих даних із застосуванням об'єктивних факторів, згаданих у вказаному Регламенті. Таким чином, застосування поміркованого підходу до поняття персональних даних може також полегшити передачу псевдонімізованих даних між суб'єктами господарювання, якщо запроваджено належні міри захисту таких даних.

Ключові слова: загальний регламент про захист даних, персональні дані, псевдонімізовані дані, ідентифікація, концепція персональних даних, абсолютний підхід, відносний підхід.

Introduction. Arguably, one of the biggest events (if not the biggest) in the legal domain in May 2018 in the European Union (hereinafter – the EU) was entry into force of the General Data Protection Regulation (hereinafter – the GDPR) [1].

Although the GDPR was not the first document regulating data protection in the European Economic Area and was built upon the pre-existing concepts in the Data Protection Directive (hereinafter – the DPD) [2], it introduced numerous novelties which shifted a paradigm of data protection in a significant manner. Yet, definition of personal data has not changed much in comparison with the DPD repealed by the GDPR.

Consequently, one could presuppose that the concept of personal data is already well examined and established in the legal doctrine, law enforcement practice and business. Unfortunately, it is far from truth. Moreover, there is no consensus among academicians and practitioners how to interpret and apply both the GDPR and case-law regarding the concept of personal data. Namely, this problem was discussed by Finck and Pallas, Hintze, Oostveen, Purtova, Reid, Spindler and Schmechel, Stalla-Bourdillon and Knight, Zuiderveen Borgesius and others.

It is evident that such a situation is alarming since personal data is a core concept in the data protection legislation. That is why this article **aims** to piece together legal rules, case-law, academic perspective, and practical implications related to the notion of personal data. In order to achieve this goal, I will first introduce a legal context. Further, I will present an overview of the academic approaches to lay the groundwork for the further discussion of the concept of personal data in the

data protection legislation at the EU level and in the *Breyer* case [3]. Finally, I will provide an algorithm to deal with this concept in practice and final conclusions.

1. Concept of personal data in the legal context

According to Article 2 (a) the DPD personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

In turn, pursuant to the GDPR personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Article 4 (1)).

As it is possible to witness, although the GDPR expanded a list of identifiers, the constituent elements of personal data remained the same. That is why I dare to assume that findings made regarding the concept of personal data in the DPD may be still applied in the GDPR context with minimum reservations.

Yet, this concept was further developed in the GDPR by introduction of pseudonomisation (Article 4 (5)), which is "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 organisational measures to ensure that the **personal data** are not attributed to an identified or identifiable natural person" (emphasis added).

Such a novelty, in turn, underlay the subsequent amendments in Recital 26 of the GDPR "[t]he principles of data protection should apply to any information concerning an identified or **identifiable** natural person. Personal data which have undergone **pseudonymisation**, which could be attributed to a natural person by the use of additional information should be considered to be information on an **identifiable natural person**. To determine whether a natural person is identifiable, 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**. To ascertain whether means are **reasonably likely to be used** to identify the natural person, account should be taken of **all objective factors**, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to **anonymous information**, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes" (emphasis added).

If to follow the GDPR perspective, data becomes personal when controller or a third party can identify the data subject by applying the "means reasonably likely to be used" [4, p. 13].

As it may be observed from the definition of personal data and is noticed by the Working Party (hereinafter – the WP), data to be qualified as the personal data is required to unite the following blocks: "any information", "relating to", "an identified or indentifiable", and "natural person" [5, p. 6]. All data that does not contain any of these blocks is not considered personal data and, subsequently, is excluded from the scope of data protection legislation.

Since the first three blocks are relatively straightforward [5, p. 6–12, 21–24; 6, p. 304–305], considering the limited space, only a block pertaining to the identifiability will be discussed in detail below. Because it has provoked an academic controversy regarding the concept of personal data.

2. Academic approaches to the concept of personal data

Among academicians, there are two approaches to the concept of personal data in relation to the indentifiability condition, namely absolute (or objective) and relative (or subjective) approaches. Finck and Pallas claim that the focus of the first approach is any third party processing data, and of the second one – only the data controller [4, p. 17]. I can agree with the researchers only to the limited extent. It is important to consider not only a person processing data but also the nature of instruments in possession of the respective person that may be applied to the processing.

Thus, adepts of the first approach argue that it is necessary to take into account all factors and chances, even theoretical ones, for identifying the data subject by controller. It means that estimating nature of data, controller is required to consider all means possible and available to any person in the world to decrypt or decode the encrypted personal data. As a result, any person who is processing the encrypted personal data even without possessing a key for decryption is subject to the data protection legislation [7, p. 165]. In other words, in terms of the pseudonomisation, as long as the key for decryption exists *per se*, the pseudonymised data will always have a status of personal data for any person involved in its processing.

The first approach is criticised by other academicians because it may lead to the world where only personal data exists and anonymisation is impossible. In addition, since the worst possible assumption is required by the absolute approach, there is no need for any types of risk management [8, p. 83]. They also argue that only realistic and practically achievable means and chances for identification of data subject should be taken into account. Consequently, in terms of the encryption generally and pseudonomisation in particular, a person is subject to the data protection legislation only if she is able to decrypt data or has reasonable chances for acquiring the decrypting key [7, p. 165–166].

Some supervisory authorities have elaborated their own moderate approaches to the concept of personal data. For example, the Information Com-

missioner's Office (hereinafter – the ICO) established the "motivated intruder" test. It is required from a recipient to estimate whether a reasonably competent, without specialist knowledge, person with access to the Internet and publicly available resources can re-identify personal data [9, p. 22–23]. In other words, although any other person is added to the equation, this person is not expected to potentially possess unlimited means.

3. Further discussion of the legislative rules on the concept of personal data

In this part of the article, I will analyze the GDPR in order to estimate the above statements.

Before conducting such estimation, I would like to remind that the right to the protection of personal data is not absolute (Recital 4 of the GDPR), and the GDPR is a piece of legislation that should be interpreted in conjunction with other legal instruments.

The EU Charter of Fundamental Rights contains apart from the rights to the respect for private and family life (Article 7) and to the protection of personal data (Article 8), also the freedoms of the arts and sciences (Article 13) and to conduct a business (Article 16) [10]. An importance of the economic growth and scientific advance as well as value of the protection of individuals are also recognised in the Treaty on EU (Article 3) [11].

Besides, despite being aimed at safeguarding natural persons' right to the protection of personal data, the GDPR itself acknowledges the value of economic progress (Recital 2).

Consequently, I would dare to assume that an interpretation of the GDPR and the notions in question should by default be rather relativistic since the right to protection of personal data must be weighed against other rights. That is why, once the sufficient level of protection of personal data is established, in my opinion, the objective of the GDPR is achieved. If measures required by the data protection authorities (hereinafter – DPA) exceed the objective set by the GDPR, then they are excessive and violates the EU legislation.

Back to the concept of personal data, in the GDPR both absolute and relative approaches to this concept may be found.

As Spindler and Schmechel note, invocation of "another person" in Recital 26 of the GDPR may be interpreted as leaning towards the absolute approach, when any person in the world should be considered. Moreover, reference to the indirect indentifiability and non-exhaustive list of identifiers in this Recital and Article 4(1) may be construed as the absolute approach [7, p. 166].

Simultaneously, such expressions as "means reasonably likely to be used" and "all objective factors" in Recital 26 substantiate the relative approach to the assessment of identifiability of a data subject [7, p. 166–167]. Also, interpreting the concept of personal data in the DPD, the WP argues that "a mere hypothetical possibility to single out the individual is not enough to consider the person as 'identifiable'" [5, p. 15].

It means that risk of identification is a demarcation line between personal data and non-personal data (the risk-based approach). Namely, when the risk of identification is reasonable, then data should be qualified as the personal data. If the risk is merely hypothetical, even not excluded completely, then data is the non-personal data [4, p. 14]. Otherwise, as it was mentioned above, anonymisation would be impossible. Yet, this concept is present in the GDPR.

Subsequently, as Purtova puts it, "[t]he resulting standard of the reasonable likelihood of identification is quite broad and context-dependent, leading to one major consequence: the status of data as 'personal' is dynamic" [12, p. 46–47].

This dynamism of the status of data does not contribute to the legal certainty. If distinction between personal data and non-personal data or anonymised personal data is rather intuitive (yet not exactly clear [13]), status of the pseudonymised data poses even more questions.

The definition of pseudonymisation in Article 4(5) of the GDPR demonstrates that data carrying the status of personal data in the beginning of pseudonymisation ends this process with the same status. The pseudonymisation is a security measure to prevent direct identification of a data subject, but not by any other means reasonably likely to be used to identify her (indirect identification) [14, p. 223]. As a result, the WP has arrived at a conclusion that pseudonymised data is covered by the data protection legislation [13, p. 3, 10, 20].

It is interesting that the ICO takes more moderate approach in relation to the former data protection legislation [9, p. 21] and to the GDPR, claiming that "[p]ersonal data that has been pseudonymised – eg key-coded – **can** fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual" (emphasis added) [15, p. 4].

It is even more interesting that the WP in its opinion on the concept of personal data providing an example on the transfer of pseudonymised data from hospital or doctor to a pharmaceutical company applies more nuanced approach to the application of data protection legislation to the pharmaceutical company. Although the WP does not explicitly exclude the pharmaceutical company from the scope of data protection legislation, neither it calls pseudonymised data anonymised for the respective company, it clearly acknowledges difference between processing this data by the hospital or doctor and by the pharmaceutical company. It states, consequently, "a Data Protection Authority may consider that no means are present in the processing performed by the pharmaceutical company" [5, p. 15–16].

Arguably, the GDPR leaves little room for maneuver for an original controller who pseudonymises data – the pseudonymised data will be personal data for her. But the question is whether a recipient of the pseudonymised data is a holder of the personal data? As Hintze notices, in case the original controller possesses both de-identified data (including the pseudonymised data) and key to it, then there are no significant obstacles for re-identification. Another situation is with the subsequent recipient of such data, for who re-identification is troublesome or unfeasible [16, p. 88]. The further discussion will be dedicated only to the status of the recipient of pseudonymised data.

If to have a nuanced attitude to the status of pseudonymised data defining whether it is person-

al or non-personal data, it is important to answer for whom and what means this person possesses. Such an approach is also in tune with the above observation regarding the concept of personal data. Otherwise, if to apply the absolute approach to pseudonymised data, it will always be qualified as personal data because potentially there is a person in the world who is capable of decrypting data in question. If to veer towards the relative approach, the pseudonymised data will be deemed as the personal data only for the controller who transfers such data.

In order to find a solution for this situation (at least to attempt), it is necessary to turn to the GDPR. At first sight, Recital 26 of the GDPR can be interpreted that pseudonymised data is always personal data. Besides, the wording "or by another person" may (and should) be interpreted as such that assessment of the status of pseudonymised data must be undertaken through the position of both the controller and a third party. Based on these assumptions, it may be concluded that the absolute approach is applied here.

However, an invocation of the "means reasonably likely to be used" limits scope of the identifiability under such means. It may be assumed that if appropriate organisational, contractual and technological measures are applied in the course of pseudonymisation of data, then such data may be anonymous in certain cases, for example, for a third party-recipient [14, p. 227; 17, p. 2].

Besides, according to Recital 26 of the GDPR these means are assessed through "all objective factors", not all possible factors. Further, since Recital 26 contains a non-exhaustive list of such factors, like the costs and amount of time required for identification, the available technology, these factors are different in each particular case. It is another hint towards the relative approach.

Thus, expressions "means reasonably likely to be used" and "all objective factors" signify that it is necessary to apply the case-specific approach in assessment of the status of pseudonymised data for a particular recipient [14, p. 228].

As Stalla-Bourdillon and Knight put it, personalisation "should not be seen as a property of the data but as a property of the environment of the data" [18, p. 312]. Consequently, reasonableness should be assessed differently for a private person or an online platform, etc. Also, a presumption of means available to such entities should differ, being limited to knowledge of these parties in the sphere relevant to the (re-) identification of a data subject [4, p. 18–19].

Here, it is necessary to introduce Hintze's position, who has not followed the named dichotomy and elaborated a spectrum of identifiability (identified, readily-identifiable, Article 11 de-identified, and anonymous/aggregate data). Considering limited space, I will just mention that all first three levels of data belong to the personal data, and the third type requires close scrutiny in relation to the discussed issues. Thus, Hintze claims that Article 11 de-identified data includes the pseudonymised data and still relates to a specific person even if the controller does not have the additional data or key for re-identification. He explains that this is the case when initial controller transfers pseudonymised data to a recipient (controller) who does not have "any practical access to any additional data" for re-identification. This is also applicable to the situation when the initial controller destroyed the additional data allowing re-identification after the pseudonymisation [16, p. 91–93].

Suggestion of the alternative approaches to the concept of personal data should be warmly greeted since the discussed rigid dichotomy (absolute vs. relative approaches) may be detrimental to the law enforcement and business. It seems, however, that a closer look at Article 11 of the GDPR ("Processing which does not require identification") is needed. First of all, Article 11 of the GDPR does not clearly operate with notions of pseudonymised or anonymised data. Secondly, according to the GDPR's definition of pseudonimisation the additional data still exists and is kept separately. Although the GDPR is silent about who keeps it separately, yet it is possible to assume that it is a person who processes data (not a data subject). Next, conclusion that may be inferred from the wording of Article 11 is that there is no identification of data subject on the part of controller who "is not in a position to identify the data subject". Subsequently, if to apply approach present in Recital 26 of the GDPR, it is possible to say that this data will be anonymous for the controller until the data subject provides additional information necessary for her identification. In this case, following Article 11(2) of the GDPR, the controller is required to perform her obligations only under Articles 15 and 20 of the GDPR, which corresponds to the approach to the anonymised data. Namely, once the controller does not possess additional information from the data subject, she cannot anymore re-identify her.

Therefore, an interim conclusion regarding the concepts of personal data and pseudonymised data is that the moderate approach, in-between the absolute and relative ones, should be applied. In other words, not only knowledge and means available to the controller but also to a third party should be considered. Yet, these means should be limited by the criterion of reasonableness.

Additionally, application of the moderate approach to the concept of personal data should be shaped in accordance with the derogations relating to processing for scientific or historical research purposes, statistical purposes, or archiving purposes in the public interest (Article 89 of the GDPR). Otherwise, arguably, application of the absolute approach to the concept of personal data may seriously stall the achievement of these purposes.

To test the suggested approach, I will turn to the case-law next, namely the *Breyer* case.

4. Concept of personal data in the Breyer case

First of all, it is important to point out that (1) the DPD is examined in *Breyer* case, and it does not concern (2) the pseudonymised data.

Consequently, findings in the *Breyer* case regarding the concept of personal data have only a persuasive power in relation to the GDPR. Besides, expansion of such findings to the pseudonymised data under the GDPR is a question of private interpretation. Nevertheless, since there are no other judgements of the Court of Justice of the European Union (hereinafter – the CJEU) available at the time of writing, this case may provide insights into

the concepts of personal data and pseudonymised data under the GDPR.

Factual background of the case is the following. Mr Breyer has filed a lawsuit before the German courts against the Federal Republic of Germany to prohibit it from storing, or arranging for third parties to store the users' IP addresses after their visits to accessible to the public websites of the German Federal institutions. In more detail, users were accessing such websites managed by the provider of online media services. As a result, 'dynamic' IP addresses of users' computers along with the date and time of accession were registered in order to prevent attacks and prosecute 'pirates'. Such IP addresses, unlike 'static' ones, change each time after a new connection to the Internet and, consequently, does not allow to establish a link between an accessing computer and connection to the network used by the Internet service provider. In such a manner, the online media services provider cannot directly identify user by the named above registered data. However, if the dynamic IP addresses are combined with the additional data available to the Internet service provider, then user may be identified by the operators of the websites [3, paras 13–14, 16–17, 24].

After the first and appeal instances this case was taken to the German Federal Court of Justice. This Court referred to the CJEU for a preliminary ruling, *inter alia*, a question whether an IP address constitutes personal data for an online media service provider if a third party (in this case an Internet service provider) possesses the additional data which enables in composition with the IP address to identify the data subject? [3, para 30].

The CJEU, as an answer to the above question, stated that pursuant to the DPD a dynamic IP address falls under the scope of definition of personal data for an online media services provider if it has the legal means to request from the Internet service provider additional data necessary to identify the data subject [3, para 65].

In order to reach such conclusion, the CJEU, in my opinion, has established a test for qualifying data as the personal data in this case. First step to take is to check whether data in question identifies natural person, then such data constitutes personal data. If it does not identify natural person, the next step is to verify whether such data relates to an identifiable natural person directly or indirectly by virtue of use of the additional data [3, paras 38–41].

In turn, verification of the identifiability of natural person consists of the following two sub-steps. First, it is necessary to consider not only the controller but also other persons related to data in question, because "it is not required that all the information enabling the identification of the data subject must be in the hands of one person" [3, para 43] (the absolute approach). Next, reasonableness of means likely used by such person to combine pieces of data available must be assessed (the relative approach) [3, paras 42, 45].

According to the CJEU position the reasonableness condition is met if identification is illegal or unfeasible because of enormous efforts required, and, as a consequence, risk of identification is insignificant [3, para 46].

Therefore, I am inclined to believe that the CJEU applied the moderate approach (in-between the absolute and relative ones) to the concept of personal data in the *Breyer* case. Indeed, on the one hand, it would be unreasonable to expect from the CJEU to exclude the absolute approach from application, since Recital 26 of the DPD also contained such wording as "or by any other person". On the other hand, the CJEU emphasised that the "means likely reasonable to be used" shall be taken into account to test identifiability of a natural person.

In turn, Zuiderveen Borgesius, emphasising the narrow scope of *Breyer* case, opines that the CJEU "favours" the absolute approach to identifiability of dynamic IP addresses since means likely reasonably to be used not only by the controller but also by any other person must be considered [19, p. 136–137].

Accepting Zuiderveen Borgesius' opinion, Purtova, however, argues that the Court's opinion is more nuanced than the broad scope of concept of personal data, read the absolute approach, suggested by the WP in its opinion on the concept of personal data. Namely, the CJEU in its assessment of means that are reasonably likely to be used, unlike the WP [5, p. 15], brings in "the factor of legality" of such means. Although Purtova herself points out that it is not that clear how to interpret this factor, it is possible to agree with her that invocation of this factor and limitation of the means in question to legal ones is a step away from the all-encompassing position of the WP [12, p. 62–65].

Reid, on the contrary, claims that the CJEU applied the relative approach to qualification of the dynamic IP addresses as the personal data. The Court admitted that the dynamic IP addresses belongs to personal data but only if a website's provider possesses legal means to access the additional data held by the respective Internet service provider [20, p. 5].

Mourby et al. also opine that the CJEU, negating the absolute approach suggested by the Advocate General, did not follow the named approach to the concept of personal data and favoured a more relative one. In absence of the discussed above legal means, data related to the IP dynamic addresses "would **not** have been considered personal simply because a known third party could identify [it]" (emphasis added) [14, p. 226].

Here, it is necessary to point out that the conclusions of Reid and Mourby et al. are not identical. And, if it is possible to find substantiation of the Reid's position in the judgement, the Court did not provide any opinions in relation to the data that does **not** constitute personal data. This differentiation is important in terms of qualification of data as personal or non-personal. That is why stretching this judgement to the concepts which have not been considered is acceptable if it is recognised that the CJEU has not made any general conclusions what is personal data and even less what is not personal data. It resolved only a particular problem with the dynamic IP addresses under the German law.

Before drawing interim conclusions, I would like to mention that Niemann and Schüßler also argue that the Court applied a more relative approach to the concept of personal data, but it did not explicitly refrain from the absolute one. Besides, they em-

phasise that respective local law provisions should be considered in assessment of the data in question on a case-by-case basis [21].

For example, right after the *Breyer* judgement the Italian Cassation Court (Corte di Cassazione Civile, sez. 3, no. 20615 of 13 October 2016) rendered a decision in a case related to the indirect identification of data subjects. It stated that in some cases even name and surname are not sufficient to deem a natural person identifiable [22].

In Finland, for instance, approach to the concept of personal data is rather absolute [23; 24]. However, to my knowledge, there are no judgements at the highest judicial level regarding the concept of personal data or pseudonymised data. That is why approach applied by the respective DPA should be assessed through the point of view of, *inter alia*, possible litigation or loss of reputation, not as the ultimate truth.

Finally, returning to the impact of the *Breyer* case on the pseudonymised data, Mourby et al., acknowledging incompleteness of the pseudonymised data (like in the named case) and similarity of Recital 26 of the DPD and of the GDPR, argue that it may be inferred from the *Breyer* case that the pseudonymised data may constitute personal or anonymous data depending on the circumstances of a particular case. Assessing these circumstances, one should take into account nature of the relationships between parties involved, whether a recipient conducting secondary use of pseudonymised data has any means reasonably likely to be used to identify natural persons. If she does not, then the data will not constitute personal data for the recipient, remaining personal data for the provider of such data [14, p. 227].

Therefore, it is necessary to reiterate that judgement in the *Breyer* case has a narrow scope – the dynamic IP addresses. The German Federal Court of Justice relied on the academic discussion regarding the absolute and relative concepts of personal data referring the case to the CJEU [3, para 25]. But the CJEU refrained from assessing these concepts. Consequently, this judgement does not contain an answer to the question what concept of personal data (absolute or relative one) should be applied, neither what data constitutes personal or non-personal data. Yet, it may serve as a guidance for substantiation of the moderate approach to the concepts of personal data and pseudonymised data.

5. Practical implications of the concept of personal data

In this part of the article, I will provide a general algorithm that may be followed in business operations related to the transfer of pseudonymised data. This algorithm should not be regarded as a legal advice.

Before presenting the algorithm, I would like to remind that, on the one hand, the right to the protection of personal data is not absolute and is required to be balanced against other rights. In other words, the EU legislation does not guarantee over-protection or supremacy of the protection of personal data in the EU. That is why it must be sufficient to apply measures that guarantee an adequate protection of personal data. On the other hand, it is important to keep in mind that this sort of approach is not necessary accepted by a DPA or courts in a certain Member State.

The following algorithm allows, in my opinion, to secure positions of the original data controller and possible recipient.

(1) Pseudonymise data according to the best techniques available to the original controller;

(2) Apply organisational, technical and other measures to separate a key from the pseudonymised data;

(3) Define nature of the relationships between the original data controller and a recipient [14, p. 225];

(4) Inform the recipient that the pseudonymised data is to be transferred;

(5) Suggest application of the absolute approach, meaning that the transferred pseudonymised data will have a status of the personal data for both the original data controller and recipient in order to secure compliance with the GDPR;

(6) In case it is not technically feasible (e.g., recipient is required to obtain consents from non-identifiable data subjects, *etc*. [25, p. 703]), or if recipient refuses to treat the pseudonymised data as personal data, define an applicable national law;

(7) Check the respective provisions of national law, decisions of a DPA and case-law regarding the concepts of personal data, including the means reasonably likely to be used to identify the natural person, and of pseudonymised data;

(8) If parties have arrived at a conclusion that there are no means reasonably likely to be used to identify natural persons available to the recipient, and applicable legislation and case-law do not favour the absolute approach, then it is necessary to put in place organisational and technical measures, along with legal obligations (e.g., contractual obligation of the recipient not to re-identify natural persons) to secure rights of data subjects [18, p. 298–299];

(9) Verify and update level and credibility of the pseudonymisation technique constantly [7, p. 173]. This monitoring obligation is paired with the requirement to adopt organisational and technical measures in response [4, p. 17].

Conclusions. Even though the concept of personal data in the GDPR is inherited from the DPD with minor changes, its interpretation varies among law enforcement bodies, academicians, and practitioners.

The academicians have divided into two groups sharing either absolute or relative approaches to the concept of personal data. Broadly, representatives of the former approach claim that this concept covers both the data controller and any third party, while in the focus of the latter approach is only the data controller. This academic debate originates from the vague wording of the EU data protection legislation and varying interpretations of the CJEU's position in the *Breyer* case.

In opposition, a moderate (or nuanced) approach may be suggested. Application of such an approach may be inferred from the legal rules embedded in the GDPR. Moreover, this approach is in tune with the values voiced by the EU when such right as the protection of personal data is required to be balanced against other rights and freedoms, for instance, to conduct business. If to follow the moderate approach to the concept of personal data, then it is necessary to consider any third person processing personal data. However, in order to claim that processed data is the personal data for this third person, it is re-

quired to assess through all objective factors whether she possesses means reasonably likely to be used for processing such data and identifying the natural person. Additionally, the moderate approach may be applied to the pseudonymised data allowing to define a legal status of the initial data controller and its recipient in a nuanced manner.

Consequently, until the concept of personal data is officially interpreted, it is possible to suggest following the moderate approach to the concept in question. Yet, it is necessary to bear in mind that disregard of the absolute approach will most likely bring additional risks to business activities if law enforcement bodies favour the named approach to the concept of personal data.

References:

1. Regulation (EU) 2016/679 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 (General Data Protection Regulation): the European Parliament and the Council of 27 April 2016. OJ L119/1.
2. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data: of the European Parliament and of the Council of 24 October 1995. OJ L281/31.
3. C-582/14 Breyer v Bundesrepublik Deutschland: Judgement of the Court of Justice of the European Union of 19 October 2016. ECLI:EU:C:2016:779.
4. Finck M., Pallas F. (2020) They Who Must Not Be Identified – distinguishing Personal from Non-Personal Data Under the GDPR. *International Data Privacy Law,* vol. 10, no. 1, pp. 11–36.
5. Article 29 Working Party. Opinion 4/2007 on the concept of personal data, WP 136. 20 June 2007. 26 p. URL: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf
6. Oostveen M. (2016) Identifiability and the Applicability of Data Protection to Big Data. *International Data Privacy Law,* vol. 6, no. 4, pp. 299–309.
7. Spindler G., Schmechel P. (2016) Personal Data and Encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 7, no. 2, pp. 163–177.
8. El Emam K., Alvarez C. (2015) A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques. *International Data Privacy Law,* vol. 5, no. 1, pp. 73–87.
9. Information Commissioner's Office. Anonymisation: Managing Data Protection Risk Code of Practice. November 2012. 106 p. URL: https://ico.org.uk/media/1061/anonymisation-code.pdf
10. Charter of Fundamental Rights of the European Union: the European Parliament, the Council and the Commission of 2012. *OJ C 326.*
11. Consolidated version of the Treaty on European Union: 2012. *OJ C 326.*
12. Purtova N. (2018) The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, vol. 10, no. 1, pp. 40–81.
13. Article 29 Working Party. Opinion 05/2014 on Anonymisation Techniques, WP216. 10 April 2014. 37 p. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
14. Mourby M., Mackey E., Elliot M., Gowans H., Wallace S. E., Bell J., Smith H., Aidinlis S., Kaye J. Are 'pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK. *Computer Law & Security Review,* vol. 34, no. 2, pp. 222–233.
15. Information Commissioner's Office. Overview of the General Data Protection Regulation (GDPR). October 2017. 44 p. URL: https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf
16. Hintze M. (2018) Viewing the GDPR through a de-Identification Lens: a Tool for Compliance, Clarification, and Consistency. *International Data Privacy Law*, vol. 8, no. 1, pp. 86–101.
17. Thompson B. (July 2016) Analysis: Research and the General Data Protection Regulation. *Welcome Trust*, 12 p. URL: https://wellcome.ac.uk/sites/default/files/new-data-protection-regulation-key-clauses-wellcome-jul16.pdf
18. Stalla-Bourdillon S., Alison Knight A. (2016) Anonymous Data v. Personal Data – False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data. *Wisconsin International Law Journal*, vol. 34, no. 2, pp. 284–322.
19. Zuiderveen Borgesius F. (2017) The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. *European Data Protection Law Review*, vol. 3, no. 1, pp. 130–137.
20. Reid A. S. (2017) The European Court of Justice case of Breyer. *Journal of Information Rights, Policy and Practice,* vol. 2, no. 1, pp. 1–7.
21. Niemann F., Schüßler L. (October 2016) CJEU decision on dynamic IP addresses touches fundamental DP law questions. URL: https://www.twobirds.com/en/news/articles/2016/global/cjeu-decision-on-dynamic-ip-addresses-touches-fundamental-dp-law-questions
22. Nespurek R., Richard O., Matysová M. (February 2018) European Union: Breyer Ruling, And Dynamic IP Addresses As Personal Data. URL: https://www.mondaq.com/data-protection/677894/breyer-ruling-and-dynamic-ip-addresses-as-personal-data
23. Karineva A. (September 2020) Key aspects of GDPR applied by Finnish DPA in two recent cases. URL: https://www.lexology.com/library/detail.aspx?g=a92cd7a4-8592-4427-a3e6-50bdceeecf40
24. Finnish Social Science Data Archive. Anonymisation and personal data. URL: https://www.fsd.tuni.fi/en/services/data-management-guidelines/anonymisation-and-identifiers/
25. Peloquin D., DiMaio M., Bierer B., Barnes M. (2020) Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data. *European Journal of Human Genetics,* no. 28, pp. 697–705.