https://doi.org/10.25143/socr.22.2022.1.114-126

Erasure and Anonymisation of Personal Data in Context of General Data Protection Regulation

Mg. iur. ***Žaklīna Ieviņa***
ORCID: 0000-0003-3686-9827
Rīga Stradiņš University, Faculty of Law, Latvia
zaklina.ievina@gmail.com

Abstract

Many controllers have a desire to be able to continue using personal data instead of deleting them after the processing purpose has been fulfilled. The discussion regularly arises whether the erasure of personal data is required by the General Data Protection Regulation (GDPR) and whether it can also happen by anonymising the data. This article examines how the GDPR regulates the two terms of "erasure" and "anonymisation" as well as what requirements are demanded by using any of these in the personal data lifecycle.

An obligation to delete personal data always requires personal data. In the case of anonymous data, erasure is not required and cannot be claimed. The question to be examined and discussed in the article is therefore: If personal data exist and there is a claim for erasure, can the obligation to erase be fulfilled by anonymising the personal data?

Such question has not yet been addressed in the case law and has only been examined to a limited extent in the literature by different authors with no exact court ruling. Some authors state that the question can be answered in such a way that an obligation to delete can also be fulfilled by anonymising the data (Dierks & Roßnagel, 2021; Taeger & Gabel, 2021); meanwhile, others consider that anonymisation cannot be considered as data erasure. The answer to this question is important because it determines whether large data processors are allowed to keep data that they would have to delete and use in anonymised form for Big Data analysis or Artificial Intelligence applications that are an integral part of the world of technology.

Keywords: anonymisation, erasure, personal data, data protection, GDPR.

Introduction

In the 21st century, as the value of information technologies is increasing rapidly, large data processors need more and more data sets to analyse them for the provision of new core points of Artificial intelligence and Big Data analysis, as well as for cost minimisation and ensuring high resistance to attacks (Primenko *et al.*, 2020). The discussion arises whether anonymisation can replace erasure in the context of the GDPR. As the specific answer has not been granted within the scope of the GDPR, in this context it is not clear whether data processors can further process personal information after it has been anonymised for different purposes. Moreover, it must be considered that personal data after data anonymisation could not be considered as personal data anymore.

The question regularly arises as to whether anonymisation can happen instead of erasure of data. This can play a role, for example, if companies still need certain data to perform historical evaluations. In some cases, certain non-personal data may also still be required to perform legally required calculations or to be able to check them retrospectively, for instance, for balance sheets.

The article examines how the GDPR regulates the terms "erasure" and "anonymisation", differences between both terms, as well as what requirements are demanded by using any of these in personal data lifecycle. As there is no specific answer provided by the case law whether data anonymisation can replace data erasure in the context of personal data within the GDPR, analysis of the literature by different authors has been studied, as well as data analysis method by analysing the context of the GDPR and the opinions of Article 29 Data Protection Working Party.

Researching the question whether personal data exist and there is a claim for erasure and whether the obligation to erase can be fulfilled by anonymising the personal data, legal norms interpretation methods such methods have been used as grammatical, historical and comparative method within several European Union member states' literature and legal norms, analyses of scientific articles from SCOPUS, Web of Science, ERIH PLUS and elsewhere.

The aim of the present study is to define whether upon personal data existing and there being a claim for erasure, the obligation to erase can be fulfilled by anonymising the personal data.

1 Term "Anonymisation" in GDPR

The GDPR does not mention or define anonymisation in any provision but assumes this form of processing in several provisions and mentions it in Recital 26 GDPR once.

Recital 26 of the GDPR states that

> "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Regulation (EU) 2016/679, Recital 26);

however, a more specific definition has not been provided. It is possible to conclude that anonymous data is the opposite of personal data. Anonymisation can be described as a method of identifiers implementation that replaces the values of personal data values with creation of a guide of conformity of identifiers with the initial data (Primenko, Spevakov & Spevakova, 2020). Thus, both terms can be distinguished from each other that anonymised personal data by the fact is not personal data. The decisive factor is that although the data contains information about a specific person, it cannot be used to establish a link to an identified or identifiable natural person.

Re-usage of personal data is important for controllers and it may be necessary to use anonymised personal data for the development of big data or artificial intelligence applications and to extract from it either statistical or general statements, correlations, behavioural patterns or decision proposals as well as to improve algorithms for building a user's profile or performance of the application. For example, a very well-known example is WhatsApp that in its Privacy Policy states that they automatically collect general location information even if the user has not chosen to use precise location-related features such as IP addresses, phone number area codes to estimate the user's general information. Once user profile has been established, the account records randomly generated identifier; it can be considered that analysis of pseydonimised information happens. Additionally, WhatsApp can be employed as a use-case when personal information is being used in a anonymised manner after the user account is deleted by stating that after deletion of the account, copies of certain log records remain in the WhatsApp database but are disassociated from personal identifiers to measure performance, reliability, and efficiency and to operate and improve the Services (WhatsApp Privacy Policy, 2022). Other controllers want to keep the data anonymised for the same purposes as the above-mentioned WhatsApp for improvement of algorithms or performance of application, etc.

In Recital 26, the GDPR specifies the result of anonymisation, it also specifies requirements for anonymisation. According to the relative concept of personal reference, it must be determined in a risk assessment, which considers both the interest of potential data processors and the means of attribution that can be mobilised by them, and whether the data remaining after anonymisation are personally identifiable. The allocation to an identifiable person turns so disproportionate in relation to the effort required for this that identification is not to be expected according to general life experience or the state of the art in science and technology. The existing or acquirable additional knowledge of the controller, current and future technical possibilities of processing, as well as the possible effort and the available time must be considered. An absolute exclusion of the assignment is neither possible nor necessary (Opinion 5/2014 on Anonymisation Techniques, 2014).

The method of anonymisation depends on the structure and content of the respective data set. In addition to the irreversible erasure of explicit or direct identifiers such

as names and addresses, personal identification numbers, and account numbers, other measures are required, such as the replacement of concrete information with generalised substitute information, or the controlled incorporation of various errors. The strengths and weaknesses of anonymisation techniques have been analysed by the *Article 29 Data Protection Working Party* on Opinion 5/2014 on Anonymisation Techniques in a more detailed way (Opinion 5/2014 on Anonymisation Techniques, 2014).

As one of anonymisation methods, a method when instead of data subject-specific data more general data are integrated can be mentioned; for example, instead of using specific city of the data subject's residence, the name of the state is used instead: instead of using Los Angeles (actual location) California (more general region) is used, or instead of using John Smith and Sara Rose, only "men" instead of John Smith and "women" instead of Sara Rose is used. The main objective of such personal data anonymisation, in this case, would be to analyse, for example, gender and region, where specific functions of the application are used more widely. In this case the objective of anonymisation would be reached as it is no more possible to identify a specific person after such anonymisation anymore.

It can be concluded that basis for anonymisation from the controller's perspective can be found in any grounds defined in Article 6 of the GDPR, with emphasis on the controller's legitimate interests, defined in Article 6 (1) of the GDPR, in case the controller has followed Data Protection Working Party's Opinion 3/2013 on purpose limitation (Opinion 3/2013 on purpose limitation, 2013). Anonymisation of personal data can be considered as a special form of data processing and requires a legal basis due to the principle of the reservation of the law (Roßnagel, 2019) a legal basis, which must essentially result from Article 6 of the GDPR (Hornung & Wagner, 2020; Roßnagel, 2021).

2 Term "Erasure" in GDPR

The term "erasure" as such has not been defined in the GDPR; however, "Right to erasure ('right to be forgotten')" has been defined explicitly within Article 17 of the GDPR. Article 17(1) grants the rights for data subject to demand from the controller to erase the personal data if any of the following cases apply

> "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)." (Regulation (EU) 2016/679, Article 17 (1))

No clear definition in the GDPR has been provided of what "erasure" means; however, within Article 4 (2) of the GDPR, it has been defined as one of the forms of data processing, stating that

> "'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" (Regulation (EU) 2016/679, Article 4(2)).

Additionally, "erasure" describes a form of action that serves to ensure that data can no longer be used and can no longer be challenged. Erasure can take place in different ways; however, the decisive factor is that it is impossible to perceive the information previously recorded in the data to be deleted (Judgement of the court in case Case-434/16, reference 55, 20 December 2017). It is not sufficient to remove a reference to certain data in a register or to overwrite the data in a file, it is necessary that the data cannot be recovered after erasure and cannot be processed in any other.

Evaluating the technical possibilities of reconstruction after insufficient attempts at extinguishment, the requirements for erasure depend on the current state of the personal data. It must irreversibly prevent information in the data from being used further. Erasure must be performed on all data carriers of the data controller and must also cover all backup copies (Hornung & Wagner, 2020). Under the conditions of Article 17 (2) of the GDPR, the obligation to delete must also be made known to other data controllers and implemented by them. The erasure concept required for proper erasure is dealt by national or any other guidelines in regard to erasure periods for personal data that may differ case by case. Absolute security cannot be demanded for complete and irreversible rendering of data unrecognisable to anyone and for an unforeseeable period of time (Hammer, 2016). However, it must be practically impossible that the data can be restored with reasonable effort.

For erasure "destruction" of the data is not required. This form of action, in addition to erasure, is described in Article 4 (2) of the GDPR and is therefore an "alternative form of processing" to erasure (Stürmer, 2020). Destruction, in contrast to erasure, means the physical removal of the data media (Hornung & Wagner, 2020). Destruction is possible, for example, by destroying the data media if one can be sure that the data was only stored on the destroyed data media (Roßnagel, 2021).

3 Differences between Terms "Erasure" and "Anonymisation"

Analysis of the terms "erasure" and "anonymisation" shows similarities but above all differences between the two forms of processing. It must, therefore, be examined whether these differences allow the conclusion that anonymisation of personal data can replace erasure and that the controller is free to decide on the replacement.

Anonymisation is not defined in the GDPR but is only described in more detail in Recital 26 of the GDPR, as described above. According to it, the principles of the GDPR do not apply to anonymous data, i.e., data that do not (or no longer) relate to an identified or identifiable natural person. The wording makes it clear that anonymous data are the flip side of personal data within the meaning of Article 4(1) of the GDPR and thus do not fall within the scope of the Regulation as described in Article 1(1) of the GDPR. Therefore, the right to erasure can only apply to personal data, not to non-personal data. In addition, erasure does not require that the data in question be "destroyed". This already follows from Article 4(2) of the GDPR, according to which, the processing of personal data includes "erasure or destruction". Therefore, on the one hand, it is possible to conclude that it is sufficient to comply with Article 17 (1) of the GDPR if the information contained in the data has been rendered unrecognisable to such an extent that the data concerned cannot be restored or can only be restored by disproportionate means. From a teleological point of view, elimination of the reference to a person is close to deletion, because the data subject is no longer considered to be in need of protection (Specht, 2017). Thus, if all personal data is deleted in the event of a claim for deletion, and only anonymous data remains with the data controller, the claim for deletion is satisfied. For example, the customer of an online store demands the deletion of his personal data. In this case, the online store will nevertheless have to ensure that it retains the non-personal data that it needs to prepare its annual financial statements, to detect accounting errors in the event of a tax audit or to analyse sales over specific periods in the past for business planning purposes.

4 Terms "Erasure" and "Anonymisation" Compared regarding GDPR

A major shortcoming of the GDPR is that it only defines the collective term of data processing and explains it with 16 data processing examples:

> "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Regulation (EU) 2016/679, Article 2).

However, in Article 4 (2) of the GDPR, there are not defined most of the above-described data processing examples or "erasure" either, for which the most specific definition can be found in Article 17 and in Recitals 65, 66 and 81 of the GDPR. Within the scope of the term "anonymisation", the same advantage can be found in scope of the GDPR because the GDPR not only does not define the term "anonymisation" but also does not mention it in the whole regulation except in Recital 26 GDPR, where it is mentioned once.

It is undisputed that both forms of processing fall under the concept of processing. Article 4 (2) of the GDPR, however, mentions erasure as a separate form of processing

because it changes the data in a very specific manner. Since it deprives the data of their further processability, it is logical to emphasise this specificity separately. Anonymisation removes personal reference of the data and thus withdraws it from the scope of the regulation. In order to distinguish it from the usual forms of processing, anonymisation should be regarded as a separate – unnamed – form of data processing (Hornung & Wagner, 2020; Roßnagel, 2021).

It is not possible to draw any conclusions when evaluating the term "processing" defined in Article 4(2) of the GDPR that states that

> "'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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Regulation (EU) 2016/679, Article 4(2))

No conclusions about any of the discussed terms under investigation can be drawn from the definition of data processing alone. "Anonymisation" is used without using the term

> "where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner" (Regulation (EU) 2016/679, Article 89),

as defined in Article 89 of the GDPR as a prerequisite for further processing of data for purposes of research, statistics, and archiving. In all cases in which these purposes can also be achieved without identifying data subjects, further processing is to take place without personal data. This is only possible if the data has been anonymised before further processing (Simitis, Hornung, & Spiecker, 2019).

Likewise, erasure of personal data is regulated very specifically in Article 17 of the GDPR. Paragraph 1 and 2 of Article 17 of the GDPR regulate obligations of the controller to erase and provide information about the data subject' s right to erasure; however, paragraph 3 of Article 17 of the GDPR determines five final exceptions to the obligation to erase. These exceptions do not include general anonymisation of data. One exception is only addressed very indirectly in Article 17 (3) (d) as a requirement in Article 89 (1) of the GDPR to further processing of the data for purposes of research, statistics, and archiving. If the Union legislator had wanted to provide for anonymisation as a general substitute for data erasure beyond this specific case, which should exceptionally exclude the data subject's right to erasure of the data, he would most probably have included it in Article 17 (3) of the GDPR. They would have done so in a similar way as in Article 89 (1) of the GDPR in relation to specific further processing. In any case, there is no indication either in the wording of the GDPR or in the conceptual use of the forms of processing that anonymisation of personal data replaces erasure (Roßnagel, 2021).

Since the GDPR does not apply to anonymised data (Regulation (EU) 2016/679, Recital 26), it can be assumed that the obligation to delete data can also be met by making the data anonymous (Hornung & Hofmann, 2013). Anonymisation does not exist; however, if the link between the data and a specific person can be restored, for example, by linking it to other data, such data is merely pseudonymised (Paal & Pauly, 2021) so that the GDPR remains applicable and the obligation to erase is not met.

5 Principle of Storage Limitation within Scope of "Erasure" and "Anonymisation"

When comparing "erasure" and "anonymisation", it must be considered that both terms can implement the principle of storage limitation defined in Article 5 (1)(e) of the GDPR (Stürmer, 2020).

The principle requires that personal data shall be

> "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (Regulation (EU) 2016/679, Article 5 (1)(e)).

This goal can be achieved both by deleting data when they are no longer necessary and by making such data anonymous. However, the fact that several measures can achieve the goal of storage limitation does not mean that they are all equivalent and can replace each other. In particular, it cannot be concluded that physical elimination of the data is equivalent to further processing of the data for another purpose, even if a personal reference is no longer required for this purpose (Der Bundesbeauftragte für den Datenschutz und der Informationsreiheit, 2020).

6 Necessary Differentiations Depending on Data Category or Any Other Condition in Case of "Erasure" and "Anonymisation"

Even if, contrary to the previous result, a substitution of erasure by anonymisation of the data were permissible in principle, this could not apply to all conceivable cases. Rather, it would be necessary to further differentiate for which erasure reasons anonymisation would be excluded and for which it would be possible. Likewise, it would have to be differentiated for which data anonymisation is possible at all, and anonymisation could be a substitute for erasure.

On the one hand, according to the grounds for a claim for erasure pursuant to Article 17(1) of the GDPR, it would have to be differentiated. No substitution of erasure by anonymisation is possible if only

> "the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject" (Regulation (EU) 2016/679, Article 17 (1)(e)).

However, this also applies if, according to Article 17(1)(d),

> "the personal data have been unlawfully processed" (Regulation (EU) 2016/679, Article 17 (1)(d)).

Otherwise, this would invite circumvention opportunities such as unlawful acquisition of data for Artificial intelligence and Big Data that can be seen as a real objective for data controllers for developing new applications and analyses tools.

On the other hand, complete anonymisation cannot be performed at all for a large number of data categories as data categories sometimes use access control of company locations such as image data of fingerprints as well as for categories such as genomic data, biomaterial samples or voice recordings. Thus, the claim that anonymisation can replace erasure should be put into perspective and exclude a significant amount of data for which anonymisation is not possible or is particularly difficult or not possible with measurable means or at least defining for which data categories anonymisation could and in which categories it could not take place, for example, splitting "personal data" and "special categories of personal data" in different possibilities of data anonymisation.

7 Different Results of Both Terms, "Erasure" and "Anonymisation"

Every anonymisation must also include erasure, namely that of identifiers at least for creating the data anonymous. As long as those are still present in the data set, the data cannot be anonymous. In this respect, anonymisation is also a partial erasure of the personal data, until the personal data cannot be considered as personal data anymore. Otherwise, anonymisation only changes the data so as not to jeopardize its further processing. In this respect, it must be questioned whether the obligation to delete can already be fulfilled with partial erasure through anonymisation or erasure must be made in a "full" manner. This must be evaluated as both forms of processing pursue different goals and achieve different results.

Erasure is intended to make stored personal data completely unrecognisable so that it can no longer be processed, read or perceived. The result of erasure is the empty data set (Pohle & Hölzel, 2020); meanwhile, in anonymisation only partly empty data set.

Anonymisation, on the other hand, aims to continue processing the data without any reference to a person but using the representation of the reality of life of the person concerned. However, the data can still be processed, read and perceived (Der Bundesbeauftragte für den Datenschutz und der Informationsreiheit, 2020). The purpose of anonymisation is for the controller to leave the scope of the GDPR and free himself from the obligation to protect the fundamental rights and freedoms of the data subjects and to safeguard the data subjects' rights as anonymised data cannot be considered personal data anymore (Pohle & Hölzel, 2020). If it were allowed to replace erasure with anonymisation, the controller could copy the anonymous data and sell or pass it on

without restriction, or use it as statistical or typing statements, correlative relationships, behavioural models or decision proposals, or other Big Data and Artificial Intelligence applications.

Anonymisation and erasure thus lead to very different results. Anonymisation cannot produce the results expected from erasure. This argues against the assumption that anonymising the data could fulfil the obligation to delete it.

The fact that anonymisation and erasure are not similar and equivalent forms of data processing is also reflected in the respective different requirements for information obligations to data subjects while conducting any activity.

While the controller must inform the data subject prior to anonymisation about the purposes and legal basis of processing for which the personal data are intended pursuant to Article 13 (1) (c), Article 14 (1) (c) and Article 14 (4) of the GDPR, these information obligations do not exist in the case of erasure as further data processing does not take place.

8 Risk Assessment Evaluation when Using "Erasure" or "Anonymisation"

Article 17(1) of the GDPR, provided that one of the six grounds for erasure applies, gives the data subject the right to require the controller to physically eliminate the data concerning them. The data subject, thus, has a right to have its risk that the data may be used against interests eliminated by the fact that it no longer exists. However, this claim to elimination of risk is defeated by anonymisation. On the contrary, the risk reduction to which the data subject is entitled is not inconsiderably increased by anonymisation for at least two reasons.

First, the risk of de-anonymisation is increased by further processing of the anonymised data (Hornung & Wagner, 2020). According to the relative concept of personal reference, anonymisation is already considered sufficient if, at the time of anonymisation, it can be reasonably ruled out that the controller can assign the data to the data subject with the additional knowledge available to him or foreseeably acquirable (Opinion 5/2014 on Anonymisation Techniques, 2014). If the data is no longer subject to data protection law under this condition, it can be passed on at any time to anyone who can process it further for a wide variety of purposes and use it, for example, for Big Data analyses and Artificial Intelligence applications. Due to dissemination of data to countless responsible parties and due to technical progress over time, the risk of de-anonymisation is continuously increasing. If the data is no longer available after correct erasure, this risk is eliminated (Roßnagel, 2021).

Advocates of the replacement option rightly point out that residual risks can remain with both erasure and anonymisation (Stürmer, 2020). This is correct insofar as data protection law allows the practical exclusion of risks to suffice for both terms "anonymisation" and "erasure". However, this commonality does not mean that both

forms of handling aim at the same level of risk or lead to the same or comparable risks. Rather, anonymisation targets a significantly higher level of risk than erasure, and proper anonymisation is much more difficult to achieve than proper erasure. Therefore, the risk to the data subject after erasure is significantly lower than after anonymisation. This also speaks against anonymisation being a substitute for erasure (Roßnagel, 2021).

Second, anonymisation preserves the data and their connections with other activities or characteristics. Although they can no longer be assigned to the person concerned, if done correctly, they still describe their relationships, characteristics, attributes, and history. When these data are later reapplied to the data subject as statistical or typing statements, correlative relationships, behavioural models, or decision suggestions, they apply to that person and may then be used against them (Weichert, 2013; Roßnagel, 2013). They enable behavioural control, especially of the individuals to whom they apply, even if the person responsible cannot identify those individuals (Richter, 2015).

Different risks after anonymisation or erasure have been also acknowledged by authors who consider anonymisation instead of erasure to be a suitable alternative, if they consider a data protection impact assessment defined in Article 35 of the GDPR to be necessary in the case of anonymisation of the data and its further use and to evaluate the possible consequences within the anonymisation made.

Despite data protection impact assessment not being required before the data is deleted, it could be considered as pre-condition in case anonymisation could replace data deletion for evaluating the possible risks to de-anonymise the data set after personal data anonymisation. This again leads to conclusion that anonymisation is associated with a significantly higher risk than direct data erasure.

Conclusions

On the one hand, the requirements defined in Article 17 (1) of the GDPR within the obligation to erase personal data from the controller's perspective cannot be seen as data erasure if anonymisation of data takes place due to the reason that two data processing methods have different goals, can cause different risks to the data subject and are also differently regulated within the context of the GDPR, the question can be indicated as crucial for the controllers concerning optimisation of applications performance and other technological improvements for development that anonymised personal data may provide.

On the other hand, in legal practice from the specific normative arrangement of the provision the obligation to erase data under the GDPR can also be seen by removing the reference to a person through anonymisation as generally Article 17 of the GDPR requires processing only that personal data which is no longer possible after data erasure. According to the above discussion, anonymisation is associated with a residual risk of re-identifiability. However, such view is based on the fact that this risk, in the case of proper anonymisation, is at least theoretically no different from the risk of identifiability of data

not initially covered by the GDPR, and thus, from the point of view of the data protection regime, anonymisation falls below the threshold of the relevant risk. Anonymisation constitutes processing within the meaning of Article 4 (2) of the GDPR, which is based on Article 6 (1) (1) (c) in conjunction with Article 17 of the GDPR.

There is no clear answer provided within the GDPR whether anonymisation can replace data erasure thus leaving space for interpretation.

Bibliography

1. Der Bundesbeauftragte für den Datenschutz und der Informationsreiheit. (2020). Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4 [rev. 07.04.2022].
2. Dierks, C., und Roßnagel, D. (2021). Sekundärnutzung von Sozial- und Gesundheitsdaten. Berlin: MWV, Medizinisch Wissenschaftliche Verlagsgesellschaft mbH & Co. KG. https://library.oapen.org/viewer/web/viewer.html?file=/bitstream/handle/20.500.12657/22455/1007726.pdf?sequence=1&isAllowed=y [rev. 07.04.2022].
3. Hammer, V. DIN 66398. *Datenschutz und Datensicherheit – DuD*, issue 8/2016, 528–533. https://doi.org/10.1007/s11623-016-0651-5
4. Hornung, G., und Hofmann, K. (2013). Ein "Recht auf Vergessenwerden"? Juristenceitung, 2(15), 163–170.
5. Hornung, G., und Wagner, B. (2020). Anonymisierung als datenschutz- relevante Verarbeitung? *ZD – Zeitschrift fűr Datenschutz*, 5/2020, 223–228. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Universität-Kassel.pdf?__blob=publicationFile&v=3 [rev. 07.04.2022].
6. Judgement of the court 20.12.2017 in Case C434/16, reference 55. *Infocuria: Case-law.* https://curia.europa.eu/juris/document/document.jsf;jsessionid=2E748703A123F58DB35405852FE05861?text=&docid=198059&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=8337338 [rev. 07.04.2022].
7. Opinion 3/2013 on purpose limitation, 02.04.2013. *European Commission. Justice and fundamental rights.* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [rev. 07.04.2022].
8. Opinion 5/2014 on Anonymisation Techniques, 19.04.2014. *European Commission. Justice and fundamental rights.* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [rev. 07.04.2022].
9. Paal und Pauly (2021). Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG.
10. Pohle, J., und Hölzel, J. (2020). Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts. *The Alexander von Humboldt Institute for Internet and Society.* https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Stellungnahmen/Alexander-von-Humboldt-Institut.pdf?__blob=publicationFile&v=3 [rev. 07.04.2022].

11. Primenko, D. V., Spevakov, A. G., & Spevakova, S. V. (2020). Depersonalization of Personal Data in Information Systems. *Springer Professional*. https://www.springerprofessional.de/de/depersonalization-of-personal-data-in-information-systems/17720882?fulltextView=true [rev. 07.04.2022].
12. Richter, P. (2015). Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data. ISBN 978-3-8487-2315-7.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 [rev. 07.04.2022].
14. Roßnagel, A. (2013). Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. *ZD – Zeitschrift fűr Datenschutz*, 562–567.
15. Roßnagel, A. (2021). Datenlöschung und Anonymisierung. Verhältnis der beiden Datenschutz instrumente nach DS-GVO. *ZD – Zeitschrift fűr Datenschutz*, 188–192.
16. Roßnagel, A. (2019). Kein "Verbotsprinzip" und kein "Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht. Juristische Wochenschrift, Issue 1.
17. Simitis, S., Hornung, G., und Spiecker gen. Döhmann, I. (Hrsg.) (2019). Datenschutzrecht: DSGVO mit BDSG: Großkommentar. Nomos. ISBN 978-3-8487-3590-7.
18. Specht, L. (2017). Das Verhältnis möglicher Datenrechte zum Datenschutzrecht. Die Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht, Issue 12, 1040–1047.
19. Stürmer, V. (2020). Löschen durch Anonymisieren? *ZD – Zeitschrift für Datenschutz*, Issue 12, 626–630.
20. Taeger, J., und Gabel, D. (Hrsg.) (2019) DSGVO/BDSG, 3. Aufl. ISBN 978-3-8005-1659-9.
21. Weichert, T. (2013). Big Data und Datenschutz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.
22. WhatsApp Privacy Policy. (2022). https://www.whatsapp.com/legal/privacy-policy-eea/?lang=en [rev. 07.04.2022].