Personal Data, Anonymisation & Pseudonymisation under European Data Protection Law

A Comparison of the DPD and the GDPR on the Example of Cloud Computing

Candidate number: 8006

Submission deadline: 01/12/2016

Number of words: 17991
Table of contents

List of Abbreviations.................................................................................................................. iii
Introduction.................................................................................................................................... 1
Methodology.................................................................................................................................. 3
1. Cloud Computing..................................................................................................................... 4
   1.1 Definition............................................................................................................................ 4
   1.2 Forms of Cloud Computing............................................................................................... 4
   1.3 Need for Legal Clarification............................................................................................... 6
2. Key-Factor “Personal Data”........................................................................................................ 7
   2.1 Personal Data under the DPD............................................................................................. 7
      2.1.1 Direct Identification........................................................................................................ 8
      2.1.2 Indirect Identification.................................................................................................... 8
         2.1.2.1 Absolute Theory....................................................................................................... 9
         2.1.2.2 Relative Theory....................................................................................................... 10
         2.1.2.3 Absolute-relative Approach..................................................................................... 11
         2.1.2.4 CJEU...................................................................................................................... 12
      2.1.3 Conclusion..................................................................................................................... 13
   2.2 Personal Data under the GDPR............................................................................................ 14
   2.3 Conclusion............................................................................................................................ 16
3. Anonymisation.......................................................................................................................... 17
   3.1 Anonymisation under the DPD........................................................................................... 18
      3.1.1 Lawful Anonymisation Process..................................................................................... 18
      3.1.2 Effective Anonymisation.............................................................................................. 20
      3.1.3 Conclusion..................................................................................................................... 23
   3.2 Anonymisation under the GDPR.......................................................................................... 23
      3.2.1 Effective Anonymisation.............................................................................................. 24
      3.2.2 Lawful Anonymisation Process..................................................................................... 26
      3.2.3 Conclusion..................................................................................................................... 27
4. Pseudonymisation................................................................................................................... 29
   4.1 Pseudonymisation under the DPD....................................................................................... 31
      4.1.1 Pseudonymisation to render data anonymous?............................................................ 31
4.1.2 Pseudonymisation as security measure.................................32
4.1.3 Conclusion..............................................................................33
4.2 Pseudonymisation under the GDPR........................................34
  4.2.1 Pseudonymisation to render data anonymous?....................35
  4.2.2 Lawful Pseudonymisation....................................................37
  4.2.3 Pseudonymisation as security measure...............................39
    4.2.3.1 Obligations.....................................................................39
    4.2.3.2 Incentives......................................................................40
    4.2.3.3 Quality of Pseudonymisation.........................................42
    4.2.3.4 Conclusion.................................................................43
  4.2.4 Conclusion............................................................................43
4.3 Conclusion–Comparison of Pseudonymisation under DPD&GDPR..44
5. Practical Impact of the GDPR for Cloud Computing..................47
  5.1 Anonymisation........................................................................48
  5.2 Pseudonymisation.................................................................49
6. Final Conclusion..........................................................................52
Table of References........................................................................54
### List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art.</td>
<td>Article</td>
</tr>
<tr>
<td>BGH</td>
<td>Bundesgerichtshof (Federal Court of Justice)</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>COM</td>
<td>Commission</td>
</tr>
<tr>
<td>DPC</td>
<td>Data Protection Commissioner</td>
</tr>
<tr>
<td>DPD</td>
<td>Data Protection Directive (The Directive 95/46/EC of 24 of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)</td>
</tr>
<tr>
<td>e.g.</td>
<td>For example</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation (Regulation (EU) 2016/679 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)</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner's Office</td>
</tr>
<tr>
<td>MS</td>
<td>Member States</td>
</tr>
<tr>
<td>No.</td>
<td>Number</td>
</tr>
<tr>
<td>OLG</td>
<td>Oberlandesgericht (Higher Regional Court)</td>
</tr>
<tr>
<td>p.</td>
<td>Page</td>
</tr>
<tr>
<td>pp.</td>
<td>Pages</td>
</tr>
<tr>
<td>Rec.</td>
<td>Recital</td>
</tr>
<tr>
<td>s.</td>
<td>Sentence</td>
</tr>
<tr>
<td>Vol.</td>
<td>Volume</td>
</tr>
<tr>
<td>vs.</td>
<td>Versus</td>
</tr>
<tr>
<td>WP29</td>
<td>Art.29 Working Party</td>
</tr>
</tbody>
</table>
Introduction

In current times of increasing use of the Internet, on-going technological developments, globalization and the emergence of a parallel online-world, data is processed in every area of life. One phenomenon of the era Internet, cloud computing, a service providing internet-based access to IT-infrastructure, applications or storage, has emerged, granting the user economical and social benefits. With cloud computing, the user has access to a cost-effective service at every time, and independently from his location.

Although such new technologies provide several advantages, concerns about data protection and data privacy have arisen more than ever. Especially in public clouds, cloud computing includes in every cloud-computing-process the uploading, combination and storing of data, that it can be assumed that cloud computing always constitutes processing what may cause high risks for the individual whose data is processed.\(^1\) Furthermore, the provision of cloud-services result in problems of lack of control, lack of information and insufficient transparency.

Those concerns may be even expanded to the question of “data protection vs. cloud computing?”. In order to challenge the new risks of data protection, there has been a need for a new suitable and more coherent regulatory framework within the EU.\(^2\)

Therefore, the General Data Protection Regulation\(^3\) (GDPR) has been approved on 14 April 2016 and will come into force on 25 May 2018.\(^4\) With repealing the current European Data Protection Directive\(^5\) (DPD), the GDPR will ensure a consistent high level of data protection and a homogenous application within all Member States, hence granting essential harmonization within the EU.\(^6\)

If the GDPR constitutes an important change to effective data protection will be discussed in this thesis concerning the different categories “personal data”, “anonymous data” and “pseudonymous data” on the example of cloud computing.

---

\(^1\) Borges/Brennscheidt, Borges/Schwenk(2012), Chap.3, p.62

\(^2\) Rec.6f. GDPR

\(^3\) Regulation (EU) 2016/679 of 27 April 2016

\(^4\) [http://ec.europa.eu/justice/data-protection/reform/index_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm); Art.94(1) GDPR

\(^5\) Directive 95/46/EC of 24 October 1995

\(^6\) Rec.10,13 GDPR
Regarding the concerns about data protection arisen in the field of cloud computing, it is important for the cloud provider, the cloud user and the individual, to clarify if data protection rules apply to cloud computing and how it can comply with those rules in an effective manner.
Under both legal frameworks, data protection rules apply if the two main criteria are met, namely “processing” of “personal data”.
Cloud computing constitutes mostly processing within the meaning under both the DPD and the GDPR, that the focus of the applicability of European data protection rules is on “personal data” as a key-factor and on the two categories of “anonymous and pseudonymous data”.
Especially in cloud computing where a huge amount of data is processed, the usage of technologies such as anonymisation and pseudonymisation are from a high relevance to exclude the processing from the scope or at least reduce the obligations.

To clarify those concerns about applicable data protection law and effective compliance, the thesis firstly gives a short overview about cloud computing in general and will further explain the need for legal clarification.
Then, to determine the application of both legal frameworks, the, in the literature highly discussed, key-factor “personal data” will be examined within a legal analysis by looking at the different theories used to consider data to be personal and at the different wording of the DPD and the GDPR.
As a possibility to circumvent the application of data protection law in cloud computing, the opposite of personal data, namely anonymous data, will be discussed by analyzing the conditions to be fulfilled in order to talk about effective anonymisation under both frameworks.
Next to anonymisation, the thesis focuses on the technical security measure “pseudonymisation”, whose implementation under the GDPR contains an important novelty, and will analyze the requirements for effective pseudonymisation and its important usefulness to ensure data security and secure processing with a comparison of both legal frameworks.
After the legal analysis of the three categories of data, the practical impact of the GDPR to cloud computing is explained within a discussion of the usefulness of anonymisation and pseudonymisation in public clouds.
Within the final conclusion, it will be summarized if the GDPR provides an important change and proper guidance in the field of different categories of data and the question if the concern “data protection vs. cloud computing?” may still be upheld will be answered.

**Methodology**

This paper shall not contain a full analysis of cloud computing and data protection. Cloud computing shall rather be an example to show the practical application of the topics discussed. Within data protection, I focus on the term of personal data as a key-factor of the applicability of data protection law. Because of the combination to personal data, I also discuss anonymisation and pseudonymisation as other categories of data and as useful security measures looking at the important changes within the GDPR.

My research is therefore based on European Data Protection Law, European case-law, Opinions of the WP29 and articles about European data protection law.

In order to assess the opinions of the WP29 and the Literature, I especially look at the wording of the law concerned.
1. Cloud Computing

Cloud Computing is a relatively new phenomenon of the era Internet as a new form of providing different IT-based services to clients online and worldwide. The term „cloud computing“ is commonly used as a slogan in the market to describe any kind of internet-based computing without defining the actual background beyond it.

1.1 Definition

In a technical view, cloud computing consists of a set of technologies and service models that focus on the internet-based use and provision of IT-infrastructure, applications, processing capability, storage and memory space in real time.\(^7\) Computing resources may be configured, expanded and accessed flexibly and location-independently on an on-demand basis with a pay-as-you-go model, depending on the actual consumption of the service.\(^8\)

In a historical sense, cloud computing may be explained as a new version of the traditional outsourcing.\(^9\)

1.2 Forms of Cloud Computing

Cloud computing can be divided into three main categories of service provision models available on the market:

With cloud computing as “**Infrastructure as a Service**”(IaaS), the basic technological infrastructure consisting of computing-, storage-, communication- and other fundamental IT-resources are provided; the user rents parts of the infrastructure of the provider, so that the latter stays the owner of a physical complex infrastructure, which is only leased to the users for a special period of time.\(^10\) An example would be the Amazon Elastic Compute Cloud(EC2).\(^11\)

The model “**Platform as a Service**”(PaaS) describes the provision of a platform, giving the user the possibility to interact and communicate for the advanced development, construction

---

\(^7\) WP196, p.4; Krcmar in Borges/Meents(2016), p.9, rec.29
\(^8\) Hon/Millard/Walden, part1,(2011), p.6; Hon/Hörnle/Millard, part3, p.3; Krcmar in Borges/Meents(2016), p.9, rec.28f.
\(^10\) WP196, p.26; Krcmar in Borges/Meents(2016), p.24, rec.20
and hosting of custom applications.\textsuperscript{12} Thereby not only the platform itself, but also all the underlying infrastructure such as additional hardware is provided.

Azure from Microsoft or AppEngine from Google are examples for PaaS.\textsuperscript{13}

The cloud as \textit{“Software as a Service” (SaaS)} provides various application services online with the benefit for the user, that the software applications do not have to be installed on the users' local system, but rather are installed on the infrastructure of the service provider that the user has to outsource the data to the provider.\textsuperscript{14} Examples are Google Mail or DropBox.\textsuperscript{15}

The functionality of those service models, but also the access to the data by the provider can be described within a three-level model with IaaS on the lowest stage, PaaS on the second level as a middle-ware-layer and SaaS on the highest stage.\textsuperscript{16}

Next to the different service models, clouds appear in different variations, depending on the way of their provision.

A \textbf{private cloud} is an IT-infrastructure which is under the exclusive control of one individual company or of a third party being strictly under the company's control and where the data is only stored within this infrastructure without being outsourced to a third party who is not under the company's strict authority.\textsuperscript{17} The access to a private cloud is strictly limited to authorized people, using mostly networks such as Intranet or Virtual Private Network (VPN).\textsuperscript{18}

In comparison to a private cloud, a \textbf{public cloud} is always offered by a third party to an indefinite number of users. The users then have to share the resources of the provider without having any control about who to share the resources with.\textsuperscript{19}

\textsuperscript{12} WP196, p.26; Borges/Brenncheidt in Borges/Schwenk(2012), Chap.3, p.47
\textsuperscript{13} Borges/Brenncheidt in Borges/Schwenk(2012), Chap.3, p.47
\textsuperscript{14} WP196, p.26; Krcmar in Borges/Meents(2016), p.27, rec.31f.
\textsuperscript{16} Hon/Hörnle/Millard, part.3,(2012), p.3; Krcmar in Borges/Meents(2016), p.26, rec.25; Eckhardt in Borges/Schwenk(2012), Chap.5, p.98
\textsuperscript{17} WP196, p.25; Borges/Brenncheidt in Borges/Schwenk, Chap.3, p.47; Mowbray/Pearson, OTM(2012), p.477
\textsuperscript{18} Krcmar in Borges/Meents(2016), p.12, rec.37; Eckhardt in Borges/Schwenk(2012), Chap.5, p.98
\textsuperscript{19} Borges/Brenncheidt in Borges/Schwenk(2012), Chap.3, p.47
Because of leaving the administration of his data to the provider, the user is bound to transfer a major portion of his control over his data to the provider.20

There are also hybrid and community clouds as mixtures or special forms of the two extremes above, picking only the advantages of private and public clouds.21

1.3 Need for legal clarification

Cloud computing, a phenomenon which cannot be seen or captured by its users, has always had a bad connotation. The user of public cloud services has to outsource his data and has – especially in cases of SaaS – transfer a major amount of his control over the data to the provider.

With the on-going development and growing of cloud computing services, multi-layered services, with lack of control and lack of transparency, has emerged, which may appear to the end user as a single service, but may in fact involve a combination of several cloud services.22

Those problems combined lead users to be concerned even more about questions of data protection, data security, transparency, control over the content and possibilities to get information about the service.

But not only the user of a cloud, also the cloud providers themselves need to know if data protection rules are applicable to their services and if they do so how to comply with those rules. According to WP29, interoperability and data portability are key-factors concerning the development of cloud computing technology but also concerning the full exercise of data protection rights, which shows a tension between cost-oriented and rights-oriented approaches.23

This possible tension can be furthermore expanded: In every cloud computing process, the user's data is outsourced, then stored or transmitted which always represents a form of data processing. This situation may lead to the question, if cloud computing can be compatible with data protection at all, in a extreme sense like „data protection vs. cloud computing?“. It is in the interest of both, the user and the cloud provider, to provide clarification about the applicability of data protection rules and how to comply with those rules within an effective manner using technological techniques.

20 WP196, p.25
21 Borges/Brennscheidt in Borges/Schwenk(2012), Chap.3, p.48; WP196, p.25
23 WP196, p.26f.
Therefore, it is important to look at the requirements of the current and the future European framework when data protection law is applicable and how to use techniques as anonymisation and pseudonymisation to possibly circumvent the application or reduce the application to a lower degree. Especially the examination of the practical impact of the GDPR in the field of personal data, anonymisation and pseudonymisation is important to provide guidance about the future applicable data protection rules. This practical impact will be discussed after a legal analysis of the categories of data under the DPD and the GDPR.

2. Key-Factor “Personal Data”

2.1 Personal Data under the DPD

The Directive 95/46/EC of 24 of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data builds the current data protection framework within the EU.

The Directive aims at the protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, but also at the free movement of personal data to establish a functioning internal market.\(^{24}\) It therefore tries to find a perfect balance between data protection and market interests.

According to Art.3(1), rec.15,17 DPD, the Directive applies if personal data is wholly or partly processed by automatic means or by non-automatic means of personal data which form part of a filling system.

The two main criteria for the applicability of data protection rules are therefore „processing“ of „personal data“.

The DPD defines „processing“ as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage.\(^{25}\)

Cloud computing mechanisms include typically the outsourcing, organization, collection and storage of data, so that by using cloud computing services, there is always „processing“ of data in the meaning of Art.2(b) DPD.\(^{26}\)

\(^{24}\) Art.1, rec.2f. DPD

\(^{25}\) Art.2(b) DPD

\(^{26}\) See1
Hence, the key-factor „personal data“ plays the important role to determine if data protection rules apply to cloud computing.

According to the definition in Art.2(a) DPD, „personal data“ shall mean any information relating to an identified or identifiable natural person(„data subject“); an identifiable person is one who can be identified, directly or indirectly[...].

With this definition, the DPD shows a broad notion of „personal data“, including not only direct identification but also indirect identification.

2.1.1 Direct identification

A person is directly identified, when the information leads to a clear and secure conclusion about the person's identity.27 A common direct identifier can be the name of a person, which most often implies a reference to a specific person. But if a name relates clearly to one individual depends on the circumstances of each case. For example: a commonly used name within a list of names about people living in one region might not allow the person to be distinguished from others, which might have the same name, but the same name might distinguish an individual in the case of a list of people within a class or neighborhood.

In the former case, the name might still be an identifier when combining the name with other information, which leads to indirect identification.

2.1.2 Indirect identification

The DPD contains with the reference to indirect identifiers a broad notion of the term „personal data“. According to the Commission, a broad definition as general as possible is important to cover all information which may be linked to an individual.28

A person is identifiable when there is no direct, clear reference to a specific person but a possibility to identify this person using a „unique combination“29 of the given information what allows the individual to be distinguished from others.

Therefore the mere possibility of combining certain information with a specific person is sufficient to talk about personal data.30

---

29 WP136, p.13
Rec.26 DPD gives a little guidance about the determination of an identifiable person: „to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person“. The criteria to be fulfilled in order to determine an identifiable person are highly disputed. Depending on the perspective which a person may be identified from, there are two extreme views, an absolute theory and a relative theory.

2.1.2.1 Absolute Theory
The absolute theory, or objective theory, takes into account all the possibilities and chances to identify an individual. It is sufficient, that a person can be identified by any person without any need that the data controller stays in contact with this person and also without any regard to costs and expenses.  

Under this theory, a data is determined to be personal looking at all possible combinations independently of the actual knowledge and ability of the controller concerned. Looking at the aims of the DPD to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy (Art.1(1) DPD), the absolute theory seems to be in accordance with the aim to protect the individuals on a very high level. This theory is also in compliance with the opinion of the Commission about a broad notion of personal data to include all information concerning an individual.

Against this objective approach, the problem lies in how to effectively perform data protection, if mostly all data can be determined as personal data. The applicability of data protection rules would be endless and an effective protection would no longer be granted. The aim of DPD is also not solely to protect the individuals but also to enable a free flow of data within the market to establish a well-functioning market. Rec.26 of the Directive also talks about „all the means likely reasonably“ which indicates that the actual knowledge, skills and costs of the controller should be taken into account in determining the identification.

32 C-582/14, 12.05.2016, rec.53; Hennrich, Cloud Computing(2016), p.128
33 See 28
35 Art.1(2), rec.3,5 DPD
Hence there needs to be a balance between the interests of individuals and the interests of the controllers. Trying to find a balance between those two interests and aims, the objective theory is incapable to come to a proper solution. Without looking at the actual knowledge, skills and connections of the controller, having no regard to the costs and expenses, the objective theory does not pay attention to the controller's interest at all which is incompatible with the provisions of DPD.

2.1.2.2 Relative Theory

In contrast to the objective theory, the relative theory or also subjective theory determines the data to be identifiable from the point of view of the controller concerned. This theory considers the necessary effort required by the controller, its actual knowledge and costs, and only realistic chances of combining information to identify an individual.36 Hence in a strict sense, data is only determined to be personal, if the controller himself is able to combine the given information in a way to identify the individual without putting an excessively effort into it.37

Contrary to the objective approach, only a limited number of data is personal data in the meaning of the DPD, which constitutes a benefit for the controller and the companies in the market. This theory also provides better evidence and clarity about the determining process, because the examination obtains only the well-known sphere of the controller.

But there might be cases where data is obviously personal by easily combining information by other people than the controller, so that it does not seem understandable to restrict the determination of data to be personal only to the sphere of the controller.

Although, according to Art.1, rec.3,5 DPD, there needs to be a fair balance between data protection and the free movement of personal data, it is incompatible with the broad definition of personal data and the intended high level of protection to restrict the protection to a very limited amount of data.

37 C-582/14, 12.05.2016, rec.53; Karg, DuD(8/2015), p.525
Looking only at the sphere of the controller is also against the wording of rec.26.\(^{38}\) Rec.26 DPD explicitly refers to means likely reasonably used „either by the controller or by any other person“ to identify the individual, which shows that the determination of data to be personal shall not be restricted in one way/view, but shall contain a broader determination to grant a high level of data protection to the individual.

### 2.1.2.3 Absolute-relative Approach

To comply with the provisions of the Directive, to find a proper balance between the interests at stake and to achieve the aims of the Directive, there needs to be a balanced theory to determine data to be personal.

„All the means likely reasonably used by either the controller or any other person“\(^{39}\) indicates, that not only the sphere of the controller is determining. The knowledge and ability of other people to combine information has to be assigned to the controller, but only in such a way that the actual costs, connections, skills of the controller concerned are taken into account.\(^{40}\)

The intended broad notion of personal data has to be limited in such a way that effective data protection can be granted.\(^{41}\)

The WP29 tends to an absolute-relative approach by stating, that „a mere hypothetical possibility to single out the individual is not enough to consider the person as identifiable“\(^{42}\)

By examining all the means likely reasonable to be used by either the controller or any other person all the factors at stake should be taken into account, such as the costs, the purpose of processing, the advantage expected by the controller, the interests at stake for individuals and risks of organizational and technical failures.\(^{43}\)

The absolute-relative approach seems to be a conciliatory solution to find a proper balance between the interests at stake and to grant effective data protection without capriciousness and less legal uncertainty.

---

\(^{38}\) Welfare, PDP(2012,12(7)), p.8  
\(^{39}\) Rec.26 DPD  
\(^{41}\) Welfare, PDP(2012,12(7)), p.10  
\(^{42}\) WP136, p.15  
\(^{43}\) WP136, p.15
2.1.2.4 CJEU

In its current decision Beyer v. Federal Republic of Germany, the CJEU has given some guidance about determining information to be personal data. The Bundesgerichtshof (Federal Court of Justice) has asked within the first question, regarding the provider of a web-page, if dynamic PI-addresses should be classified as personal data if a third party, the Internet access provider, has additional data which combined with the IP-address can identify the individual visiting the web-page.

First, the CJEU has stated clearly, that static IP-addresses, in contrast to dynamic IP-addresses, are “invariable and allow continuous identification of the device connected to the network”.

Then the court has made clear, that dynamic IP-addresses themselves, do not constitute information as an direct identifier, “since such an address does not directly reveal the identity of the natural person[...]]”.

The important guidance given by the CJEU is whether to determine indirect identifiers to be personal with the use of the absolute or relative theory.

The Advocate General has given the opinion, that rec.26 DPD should be interpreted systematically with the meaning of all the means likely reasonably used “by certain third parties”. Not only the “means” within rec.26 DPD should be likely reasonably, but also the third parties “who, also in a reasonable manner, may be approached by the controller”.

He therefore provides an objective-relative approach, arguing that within the objective theory, there would be always a hypothetical third party, “no matter how inaccessible” to the controller, which could identify the individual by combining the IP-address with additional information.

Looking at Art.2(a) DPD in accordance with rec.26, the CJEU has stated that a solely relative theory to determine data to be personal would be insufficient, arguing that the wording

---

44 CJEU, C-582/14, 19.10.2016
45 See44, rec.36
46 See44, rec.38
47 C-582/14, 12.05.2016, rec.67
48 See47, rec.68
49 See47, rec.68
“means likely reasonably to be used either by the controller or by any other person” does not require all the information to be in the hands of the controller.\textsuperscript{50}

Following the opinion of the Advocate General, the CJEU uses an absolute-relative approach to determine information to be personal data by stating that the possibility to combine the information with additional data must be likely reasonably.\textsuperscript{51}

As an argument against the absolute theory, a hypothetical risk of identification can be in reality insignificant in cases where the identification of the individual is “prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort”\textsuperscript{52}

With this decision the CJEU has finally given some guidance within the highly disputed field of determining information to personal data by showing that the best analysis, in accordance with Art.2(a) and rec.26 DPD, may be reached by using the combination of both theories within an absolute-relative approach.

\textbf{2.1.3 Conclusion}

In conclusion, under the DPD, information may be personal data not only in cases of direct identification by clearly referring to one specific individual, but also in situations of indirect identification by combining the given data with additional information which then may refer to the person concerned. In assessing when there is indirect identification according to Art.2(a) DPD, rec.26 in combination with an absolute-relative approach in the literature and currently also in the opinion of the CJEU gives a proper guidance. Hence indirect identification of an individual is considered to be given, when all the means likely reasonably used by either the controller or any other person lead to a reference to the specific individual, but only to that extend of a reasonable manner regarding the actual costs, expenses, connections and appropriate efforts of the controller. A hypothetically reference to the individual is therefore not enough to be sufficient as an indirect identification within the meaning of Art.2(a), rec.26 DPD and by combining the two views of absolute and relative theories, the “middle-way”-approach takes all interests at stake into consideration and finds a suitable balance in each case.
2.2 Personal Data under the GDPR

On 25 May 2018 a new data protection framework within the EU will come into force, Regulation (EU) 2016/679 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 (General Data Protection Regulation).\(^{53}\)

The GDPR will repeal the DPD (Art.94(1) GDPR), and will be, due to its legal form of a Regulation, binding to and directly applicable in all Member States (MS) of the European Union.

Because of the increasing use of the Internet, the on-going development of technology, globalization and the emergence of an “online-world” with an increased use of data with phenomenons like Big Data or the Internet of Things, there has been an urgent need to establish a proper data protection framework targeting new legal problems of this “online-world”.\(^{54}\)

The aim of this Regulation is to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the EU.\(^{55}\)

Challenging the problems of legal uncertainty and inconsistent application of the DPD, the GDPR fosters the consistent and homogenous application of its rules within all MS.\(^{56}\)

Because of the very broad territorial scope of the Regulation (Art.3 GDPR), it is important to look at the material scope whether data protection rules are applicable or not.

Beside the exceptions in Art.1(2) GDPR, the Regulation applies, as the DPD, to the processing of personal data of living natural persons wholly or partly by automated means and to other processing than by automated means which form part of a filing system.\(^{57}\)

The two main criteria remain the same, “processing” and “personal data”.

The definition of processing has been changed only slightly, so that the mechanisms of cloud computing still constitute a form of processing within the meaning of Art.4(2) GDPR.

Therefore, attention has to be given to the key-factor “personal data”.

According to Art.4(1)(a) GDPR personal data shall mean any information relating to an identified or identifiable natural person (data subject), which is the same wording as in Art.2(a) DPD. The definition of an identifiable natural person in Art.4(1) GDPR has been changed a

\(^{53}\) Art.99(2) GDPR

\(^{54}\) Rec.6f. GDPR

\(^{55}\) Art.1, rec.10,13 GDPR

\(^{56}\) Rec.10 GDPR

\(^{57}\) Art.1(1), rec.14f.,27 GDPR
little by adding the reference to an identifier such as a name, location data or an online identifier and a genetic factor.

Considering indirect identification, rec.26 GDPR gives further guidance. In accordance with rec.26 DPD, to determine whether a natural person is identifiable “account should be taken of all the means reasonably likely to be used […] either by the controller or by another person”\(^{58}\).

Rec.26 GDPR further explains the term “means reasonably likely to be used” with reference to all objective factors such as the cost of and the amount of time of the identification process.

Talking about all the means used by the controller or by another person to identify the natural person directly or indirectly, rec.26 seems to provide a broad and objective approach. But with clearly stating, that only means which are reasonably likely to be used shall be determining, and with thereby taking into account all objective factors such as the costs and the amount of time of the identification process or the available technology at the time, the GDPR tends to limit the broad notion by introducing an absolute-relative approach.\(^{59}\)

Although one could argue that “all objective factors” would further constitute an indication of an objective approach, there is the need to read this part of rec.26 in combination with the former sentence of rec.26. Therefore all objective factors are determining-requirements to establish some clarity in the determination-process, but should never the less be read together with “all the means likely reasonably”, which shows a relative aspect such as all objective factors “in a reasonable manner”.

Furthermore, it is not reasonable why data shall fall under the scope of the GDPR although there is no actual potential risk for the individual concerned.\(^{60}\) Applying the GDPR to all somehow possible identifiable data would lead to an endless application what would no longer grant effective data protection.

The assumption of an objective-relative approach can be further supported by looking at the aim of the Regulation: not only the fundamental right of data protection shall be ensured, but

\(^{58}\) Rec.26 GDPR


\(^{60}\) Schreiber in Plath BDSG/DSGVO(2016), p.975
also the functioning of the internal market with regard to the free flow of personal data, which indicates that there needs to be a proper balance between all interests at stake.\footnote{Art.1(1), rec.2ff.,10 GDPR}

In addition, rec.4 GDPR explains, that the right to data protection is not an absolute right, which must be considered in relation to its function in society and be balanced against other fundamental rights.

To achieve such proper balance between all interests at stake, the GDPR contains a suitable solution in determining data to be personal by looking at all the means reasonably likely to be used and by taking into account all objective factors in a reasonable manner. This balancing factor indicates the sense of an absolute-relative approach within the GDPR.

With the new wording of Art 4(1) and rec.26, the GDPR describes now as binding law the highly discussed method to determine information to be personal in the sense of an absolute-relative approach. It can be assumed that there will be less discussion about the method to be used in determining personal data and that an absolute-relative approach should be seen as the best solution.

2.3 Conclusion

Because the process of cloud computing always constitutes a form of “processing” both within the meaning of DPD and the GDPR, attention has to be drawn to the key factor “personal data” to examine the possible applicability of data protection rules to a cloud computing service.

In determining information to be personal within the sense of indirect identification, account should be taken to all the means likely reasonably to be used by either the controller or another person but only to that extend as objective factors show that there is no legal prohibition, practical impossibility or a disproportionate effort at the controller's side.

With the help of systematical interpretation of the wording of the rules within both frameworks and with the guidance currently given by the CJEU, the question whether information might be personal data shall be examined under both legal frameworks with an absolute-relative approach, reaching thereby a proper solution by balancing all the interests at stake. The GDPR therefore gives with Art.4(1) and rec.26 proper guidance and a bit more legal clarity by manifesting one theory of the literature and the opinion of the CJEU by providing the objective-relative approach within a legal framework.
3. Anonymisation

In cloud computing, a massive amount of data is processed so that it is difficult, time-consuming and costly to determine prior to every processing if there is personal data. A possible solution could be to anonymise the data prior to the processing. Anonymisation of data in general describes a technical process with the aim of irreversibly preventing the identification of individuals, whereby identification does not only mean the possibility of direct identification, but also includes potential identification by singling out, link-ability and interference. Data may be considered to be anonymous when it does not allow identification of the individual and when re-identification is not possible. There are a number of techniques included in producing aggregated information without any reference to information of an individual. Those techniques can be divided broadly into two categories of “randomization” and “generalization”.

Randomization-techniques alter the veracity of data to remove the strong link between data and individual. Using those techniques (e.g. noise addition, permutation, differential privacy), concrete numbers and identifiers will be documented in a broader sense to provide data which remains true to only a certain degree or specific information of an individual will be shuffled and artificially linked to different data subjects, that data which is sufficiently uncertain will no longer refer to the specific individual. Generalization consists of a process to generalize or dilute specific information about an individual by modifying the respective scale or order of magnitude which may prevent effectively the risk of singling out an individual. Such techniques include mainly the grouping of specific data with at least k-other data subjects (k-anonymity). This technique may then be further extended by adding to a group of equal information at least l-different values (l-diversity) or by expanding this group with t-additional parameter (t-closeness).

62 DPC Ireland, Anonymisation and pseudonymisation, p.1; WP216, p.10; Brimsted, PDP(2014,14(7)), p.5
63 Esayas, EJLT, Vol.6, No.2,(2015), p.4
64 WP216, p.12; DPC Ireland, Anonymisation and pseudonymisation, p.7; Burton/Hoffman, WSGR Data Advisor(09/2015), p.2
65 WP216, p.12ff.; Marnau, DuD(7/2016), p.429
66 WP216, p.16; DPC Ireland, Anonymisation and pseudonymisation, p.8
67 WP216, p.16; Burton/Hoffman, WSGR Data Advisor(9/2015), p.2
68 Marnau, DuD(7/2016), p.429; WP216, p.18
3.1 Anonymisation under the DPD

The DPD explains anonymous data to be the opposite to personal data with the consequence that the Directive is not applicable in cases of anonymous data. According to rec.26 DPD, “the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable”. Anonymous data which does not refer to any personal information falls therefore not under the scope of the DPD.

Hence, anonymisation-techniques could be a possible solution for cloud computing providers and users to “escape” from the obligations under the data protection framework, but also to protect the personal information of the individuals. The cloud computing provider would benefit into two different directions regarding legal obstacles and the consumers' confidence in cloud computing.

The question is then, how to provide appropriate anonymisation within the meaning of rec.26 DPD.

3.1.1 Lawful Anonymisation Process

Within the DPD there is no proper guidance about the actual anonymisation process. According to the WP29, the anonymisation process itself has, first of all, to be lawful.

Using an anonymisation-technique, data will be collected, combined, erased and stored, which constitutes “processing” within the meaning of Art.2(b) DPD. The data which shall be made anonymous has usually been collected or recorded on an earlier stage, that the anonymisation-technique falls under the concept of “further processing”, so that, in principle, the provisions of Art.6 and 7 DPD have to be met.69

But looking at the provision of Art.6(1)(e) DPD, there is an obligation to the controller to keep personal data in a form which permits identification for no longer than necessary, which shows that the anonymisation process may be compatible with the original purpose, Art.6(1)(b) DPD, and hence lawful further processing.

According to the WP29, anonymisation as further processing can be considered to be compatible with the original purposes of the processing but only on condition to reliably produce anonymous information.70

69 WP216, p.7; DPC, Anonymisation and pseudonymisation, p.8; Brimsted, PDP (2014,14(7)), p.4
70 WP216, p.7
Hence, anonymising personal data for a purpose not compatible with the original one needs to be legitimate within the meaning of Art.7 DPD to prevent violation with the data protection framework.

Criticizing the narrow view of anonymisation of the WP29, Opinions in the literature talk about anonymisation as something different or more than a compatible use, constituting mandated compliance measures and say therefore that anonymisation does not constitute further processing which therefore does not have to be legitimate itself.\textsuperscript{71}

Determining anonymisation as an privacy-enhancing technique, which generally does not threaten the individual's rights, the Information Commissioner's Office(ICO) of the UK shares the opinion, that in the absence of any unwarranted damage or distress resulting from anonymisation, there is no need to justify the process of anonymisation itself.\textsuperscript{72}

But even when following the opinion of the WP29, that anonymisation constitutes always further processing and has, if the original purpose is exhausted, to be legitimate in the meaning of Art.7 DPD, the anonymisation process mostly might, in the cases of anonymisation as compliance measures with data protection rules or anonymisation as additional security measures, e.g. regarding Art.17(1) DPD, legitimate on the ground of legitimate interests of the controller/third party in the sense of Art.7(f) DPD.

Art.17, rec.46 DPD requires the controller to implement appropriate technical and organizational measures to protect the personal data with regard of the security of processing. To comply with this obligation, controllers may use anonymisation as an appropriate technical measure, that this use of anonymisation with the purpose to comply with Art.17 DPD, would form legitimate interest of the controller within the meaning of Art.7(f) DPD. Hence, the anonymisation-technique itself as further processing would be lawful under Art.7(f) DPD.

The general assumption of the WP29 seems also more appropriate regarding legal clarity by stating that in general anonymisation constitutes further processing and has to be legitimate. When following the opinion of the literature and the ICO UK, there is always the problem to


\textsuperscript{72} Esayas, EJLT, Vol.6. No.2,(2015), p.5
determine if the special anonymisation process poses unwarranted damage or distress in regard to the individual which may be difficult and can lead to legal uncertainty. In consequence, the anonymisation process first has to be lawful in accordance with the DPD by either being compatible with the original purpose or legitimate under the grounds of Art.7 DPD.

3.1.2 Effective Anonymisation

Next to the obligation to render data anonymous within a lawful process, anonymisation has also to be effective. Effective anonymisation shall mean that data is rendered anonymous irreversibly without the possibility of re-identification, rec.26 DPD. The technology is developing fast and mechanisms of re-identification are growing constantly, what leads to the problem that it is impossible to say if a particular anonymisation-technique might be 100% effective because there might always be a possibility to re-identify anonymous data.\(^73\)

This problem raises the question about the threshold of an appropriate level of effective anonymisation to talk about anonymous data within the meaning of rec.26 DPD. Because of the congruent requirements of personal and anonymous data and because anonymous data can be seen as the opposite of personal data, attention has to be drawn again at rec.26 DPD with the focusing on “all the means likely reasonably used by either the controller or any other person” to assess if there is possible re-identification.

Under the objective theory, data might only be anonymous, if there would be no possibility of re-identification in general. Potential identification includes as typical risks of anonymisation singling out, link-ability and inference: Singling out shall mean the possibility to distinguish the information of one specific individual from all other information in one data-set; Data linking describes the possible identification by receiving information of an individual with looking at the linked identifiers in one data-set, the more identifiers are linked together, the easier it gets to identify a person;

\(^73\) DPC Ireland, Anonymisation and pseudonymisation, p.1,5; Esayas, EJLT, Vol.6 No.2,(2015),p.8; Härting, NJW(2013), p.2065,2069
Inference is understood as to link information of a data-set which is, in contrast to data linking, not originally linked.\textsuperscript{74}

Those risks in combination with the constantly evolving techniques and possible linkable data in the hands of any other person show that true irreversible anonymisation with no possibility of re-identification is unattainable under the absolute theory.

As a consequence, there would never be the situation of data not falling under the scope of the Directive.\textsuperscript{75}

This solution does not seem to be the intention of the legislator. With explicitly stating the possibility that data may be made anonymous with the consequence of no applicable data protection rules to such data, the legislator intended to grant effective data protection in such a way, that only the data which imposes high threats on the individual falls under the scope of the framework, but not also all data which is processed in a manner that usually involves very low risks of threatening.

Also, if no anonymous data would be excluded from the data protection rules, there would be no sense and no incentive for the controller to use anonymisation, what might also not be in the intention of the legislator.

Hence, the level of effective anonymisation should be determined within the absolute-relative theory.\textsuperscript{76}

The WP29 uses for this determination the “means...reasonably to be used test” to assess whether the anonymisation process is “sufficiently robust”, whether the identification has become “reasonably” impossible.\textsuperscript{77}

Such kind of anonymisation when there is theoretically a possibility to re-identify the individual, but it is practically and actually impossible to re-identify the person because of an excessive effort, is also called within the literature “de-facto-anonymity”.\textsuperscript{78}

\textsuperscript{74} WP216, p.10; DPC Ireland, Anonymisation and pseudonymisation, p.1,4
\textsuperscript{75} Härtling, NJW(2013), p.2065; Borges in Borges/Meeents(2016), p.219 rec.26
\textsuperscript{76} See 2.1.2.3
\textsuperscript{77} WP216, p.8; WP136, p.21
Within the test of sufficiently robustness, the degree of possible risks and their potential impact on the individual concerned might be an indication if the anonymisation process is effective in the meaning of rec.26 DPD.79

Also the ICO UK describes anonymisation as the “process of turning data into a form which does not identify individuals and where identification is not likely to take place”80.

Where the risk of identification seems to be sufficiently realistic, the information should be considered to be personal.81

Anonymous data with only a low risk of identification may be acceptable and so outside the scope of data protection rules. Anonymous data processed within an effective anonymisation-technique being sufficiently robust with only an acceptable degree of possible risks of identification might be determined to be anonymous data in the meaning of rec.26 DPD.

Therefore, “de-facto-anonymity” is given in such situations, when there are an excessively high effort or serious disadvantages on the side of the controller cumulative caused by the actual costs, the legal and technical restrictions to identify the individual, that it would be unreasonable within an objective evaluation to tolerate those restrictions in relation to the intended purpose.82

But bearing in mind the on-going growth and development of technology, the effectiveness of the anonymisation process should not only be determined within the current state of technology but also within the state of technology of the future, when periodically re-assessing the robustness of the specific anonymisation process.83

79 DPC, Anonymisation and pseudonymisation, p.4f.; Esayas, EJLT, Vol.6 No.2,(2015), p.7; Oswald, PDP, (2012,13(2)),p.4; Fischer-Hübner, Chap.4, p.113
81 Hon/Millard/Walden, part1,(2011), p.41,44; Esayas, EJLT, Vol.6 No.2,(2015), p.7; Oswald, PDP, (2012,13(2)), p.4
3.1.3 Conclusion

Under the DPD, data which has been rendered anonymous effectively is outside the scope of the Directive according to rec.26. Anonymisation-techniques could provide benefits to the cloud provider, the cloud user and to the individual to whom the information relates. Cloud user and cloud provider would no longer process personal data and would not have to comply with all the data protection rules of the DPD, the interest of the individual to protect its privacy would be granted and the people's confidence in cloud computing would be supported. But using any kind of anonymisation does not automatically mean an exclusion of data protection rules: the anonymisation process itself has to be lawful and the technique has to be effective within the meaning of a “de-facto-anonymity”, regarding the current state of technology and the technology in the future by constantly revising the robustness of the used anonymisation mechanism. In determining the effectiveness of a specific anonymisation-technique if re-identification is likely possible, account should be taken to an absolute-relative approach looking cumulative at the actual costs, expenses and possible excessive efforts and to the degree of possible risks of re-identification whereby an adequate low risk might be acceptable within the meaning of effective anonymous data.

3.2 Anonymisation under the GDPR

Looking at the discussions and different opinions about examining anonymous data in delineation of personal data, one could guess that the new data protection framework would give further guidance about this problem by including anonymous data within the definitions, stating the preconditions to be fulfilled in order to talk about anonymous data and by showing how to determine data to be anonymous to differentiate between the categories of data. But anonymous data is neither mentioned within the definitions of Art.4 GDPR nor within another Article of the Regulation. Similar to the DPD, a definition of anonymous data is only included within the recitals of the Regulation. Rec.26 GDPR says that anonymous information shall be “information which does not relate to an identified or identifiable natural person” and in order to talk about anonymous data, data shall be “rendered anonymous in such a manner that the data subject is not or no longer identifiable”. The Regulation excludes to the same degree as the DPD anonymous data from the
scope of the data protection principles, but clearly states in addition, that the processing of anonymous information is not concerned by the GDPR.\textsuperscript{84}

The essence of rec.26 GDPR remains the same as rec.26 DPD by talking about anonymous data as the opposite of personal data and therefore making the applicability of data protection rules dependent of the quality of the data to be either anonymous or personal.\textsuperscript{85}

With the two different explanations of anonymous information and data rendered anonymous, the GDPR shows the different situations in which information is anonymous from the beginning but also in which data has at first been personal but then may be excluded from the scope by render this data to anonymous data.

It therefore clearly points that personal data shall be at first processed within the data protection rules and principles but then may be further processed outside the scope of the GDPR on condition that this data has been rendered anonymous effectively.

\textbf{3.2.1 Effective Anonymisation}

When to talk about anonymous data within the meaning of rec.26 GDPR, the Regulation refers to the determination if data may relate to an identified or identifiable person. Hence, also under the GDPR, there needs to be the “identifiable test” to determine anonymous data in distinction to personal data.

As stated above, the GDPR uses an absolute-relative approach to examine data to be personal, so that the same approach shall also be used to indicate anonymous data.

By bearing in mind the on-going and fast developments and changes in the technology, absolute anonymisation at the current days and even more in the future is no longer achievable. With the possibility of anonymisation of data in the GDPR, which is going to be the future data protection framework in times of even faster technological developments, the Regulation shows another “hint” of an absolute-relative approach, because effective anonymisation may no longer be achievable under the absolute approach.\textsuperscript{86}

So according to rec.26 GDPR to determine an appropriate level of anonymisation, account needs to be taken to all the means reasonably likely to be used, by either the controller or an-
other person whereby in order to assess those means the GDPR requires to look at all objective factors such as costs, required time and available technology.

Within the objective factors, the GDPR considers not only the state of technology at the current time but also technological developments. A controller has therefore, in assessing if the anonymisation-technique concerned is effective, to consider technological developments, possible changes within the technology and to constantly check its anonymisation-mechanism.

Hence, the GDPR has recognized the problem of effective anonymisation in accordance with on-going changes in the technology which has already been discussed in the literature and by the WP29 under the provisions of the DPD, and goes one step further by stating this need to look at technological developments within a written form of a legal text.

By following an absolute-relative approach to determine data to be personal or anonymous with looking at all the means reasonably likely, all the objective factors (economical, legal and technological) and at the appropriateness between the actual effort to re-identify the individual, the purpose of the processing and the data protection principles, also the GDPR tends towards anonymisation within the meaning of “de-facto-anonymity”.

Talking about technological developments and anonymisation, “de-facto-anonymity” seems to be the proper solution of determining effective anonymisation, because this view of anonymisation is not static: with the exponential development of technology, the required costs and effort of re-identification may be reduced so that the relevant appropriateness may be on a case-by-case basis different in the future, that at a later stage current effective anonymisation may no longer be effective. Hence with its flexibility, “de-facto-anonymity” constitutes a solution of determining effective anonymisation at the current time but also in the future.

---

87 Rec.26 GDPR
88 See 76,78
89 WP216, p.9; WP29, WP136, p.15
3.2.2 Lawful Anonymisation Process

Similar to the DPD, the GDPR contains no proper guidance about the anonymisation process itself. Rec.26 GDPR shows two situations where either the information is anonymous from the beginning or is rendered anonymous at a later stage. But without stating conditions about the anonymisation process, the recital only focuses on the outcome of anonymisation, namely that the data subject to whom the data relates is not or no longer identifiable.92

The process of anonymisation-techniques includes as mentioned above the collection, the storing, the combination and the erasure of data which could constitute a form of processing under the GDPR.

The GDPR defines “processing” within Art.4(2) as any operation performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring[…]. Therefore anonymisation-techniques fall within this definition.

With an anonymisation-technique, personal data will be rendered anonymous with the use of processing, that the anonymisation process itself generally should fall under the scope of the GDPR. This means, that anonymising personal data needs to be done in accordance with the provisions of the GDPR.

This conclusion may also be drawn by looking at rec.26 GDPR. In its last sentence, the recital expressly excludes the processing of anonymous data, which indicates in argumentum e contrario that the anonymisation process itself shall be conducted in accordance with the GDPR and not be excluded from the scope of the Regulation.

Also one could argue that applying the rules of the GDPR to the process of anonymisation would “discourage the use of anonymisation as a privacy-enhancing technique”93 and would therefore go one step backwards regarding effective data protection, there are several possibilities to conduct lawful anonymisation according to the provisions of the GDPR.

At first, anonymisation may be lawful as “further processing” within the meaning of Art.5(1) (b), rec.50 GDPR, if the purposes of the further processing are compatible with the original purposes of the initial processing. In such cases, no separate legal basis concerning the further processing is required, rec.50 GDPR.

---

92 Rec.26 GDPR
This provision is similar to the provision of possible further processing under Art.6(1)(b) DPD, but with Art.6(4) GDPR the GDPR provides more guidance regarding the “compatibility-test” if the purpose of further processing might be compatible with the original one by taking into account any link between the purposes, the context of the data collection, the nature of the data, possible consequences of the intended further processing and the existence of appropriate safeguards.

Further, if the purpose of the anonymisation process should not be compatible with initial processing purpose, anonymisation may still be legitimate under Art.6(1)(c) and (f) GDPR. Art.6(f) GDPR, the legitimate interest of the controller, may be read together with for example rec.49 GDPR, whereby ensuring information security or preventing unauthorized access – which would be the goal of anonymisation – constitutes a legitimate interest of the controller, that Art.6(1)(f) GDPR would be fulfilled. Art.6(c) GDPR shows that processing data might be lawful if it is necessary for the compliance with a legal obligation to which the controller is subject to. Looking at the new obligations of the GDPR addressed to the controller, there are provisions including the obligation to implement technical safeguards such as Art.24(1) or Art.46(1) GDPR.

Those provisions stating the conditions of lawful processing show that requiring the anonymisation process itself to be lawful under the GDPR may not discourage the use of anonymisation or keep the controller from anonymising personal data, because there are several possibilities to “easily” determine the anonymisation-technique to be lawful.

In addition, the GDPR gives rather incentives to use anonymisation as a technical safeguard measure and hence spur the controllers and processors to take steps to more effective data protection.

3.2.3 Conclusion

Like the DPD, the GDPR also only contains a definition of anonymisation within the recitals. Although the technology is under an on-going development and the discussions about effective anonymisation within the meaning of the law rise, the new data protection framework does neither provide a proper definition within its Articles nor does it give clear provisions about the anonymisation process.
Within rec.26 GDPR, next to the definition of anonymous data, the GDPR only focuses on the outcome of the anonymisation process than rather on the conditions of the anonymisation process itself.

Similar in the main principle about anonymisation, the GDPR also talks about anonymous data as the contrary part to personal data with the consequence, that the Regulation does not apply to anonymous data.

In determining the appropriate level of effective anonymisation, account needs to be taken to all the means likely reasonably considering all the objective factors – also new technological developments in the future – to show that the information concerned does no longer refer to an identifiable individual.

With looking at objective and relative factors, the GDPR follows the modified theory, the absolute-relative approach to determine data to be personal or anonymous.

With clearly stating the need to consider also the technological developments in the future which leads to a need to constantly revising the anonymisation-technique, the GDPR modifies an unwritten and discussed condition to a written legal provision which gives further guidance in assessing effective anonymisation.

Next to the question effective anonymisation in the meaning of “de-facto-anonymity”, the anonymisation process also should be lawful within the provisions of the GDPR.

Anonymising personal data constitutes further processing, which may be lawful because of compatible purposes with the initial processing or under the legitimate interest of the controller. This legitimate interest to anonymise personal data may be given in most of the cases, either in relation to rec.49, which clearly states, that information security and preventing unauthorized access constitutes legitimate interest of the controller, or within the legal obligations within the GDPR to implement technical safeguard measure, which is usually also in the interest of the data subject.

All together, the new data protection framework, regarding the concept of anonymisation, remains in principle similar to the DPD. Anonymous data falls outside the scope of the Regulation and in order to assess data to be anonymous, the focus lays on the test if an individual may be identified or identifiable.
With adding some conditions in rec.26, the GDPR provides a bit more guidance about anonymous data, but still, the anonymous process itself needs to be lawful within the provisions of the legal framework.

But with providing a better guidance than the DPD in connection with new obligations to implement technical safeguards and security measures, the GDPR creates incentives to use anonymisation-techniques, which goes one step further to effective data protection.

4. Pseudonymisation

Next to anonymisation there is the possible technical measure of pseudonymisation.

It is important to note, that pseudonymisation does not constitute a sub-form of anonymisation, but it rather forms a separate method with another outcome.

The aim of anonymisation is to render data anonymous in a manner that the individual to whom the data relates is no longer identifiable. The connection to the individual shall be completely eliminated and re-identification shall be prevented.

On the contrary, pseudonymisation focuses on the reduction of link-ability of a data-set to not eliminate identification but rather to complicate it. In order to reduce the link-ability, pseudonymisation involves the replacing of names or other identifiers by a pseudonym such as numbers, codes or signs. A pseudonym may be further defined as the code which is used to replace the identifier in a manner that direct identification to the individual is no longer possible. Hence pseudonyms build a form of indirect identifiers.

Especially in regard to data protection, there is the need to distinguish pseudonymisation from anonymisation, because it only provides a “limited protection” for the individuals as it still allows, in many cases, the possibility of identification or relation to the data subject.

According to the WP29, pseudonymisation as such “is a useful security measure but not a method of anonymisation”, because it only reduces the link-ability to the data subject and does not eliminate such reference.

95 WP216, p.20; Hon/Millard/Walden, part 1,(2011),p.17; DPC Ireland, Anonymisation and pseudonymisation, p.1
96 WP136, p.18
97 DPC Ireland, Anonymisation and pseudonymisation, p.1
98 WP216, p.20
Typical pseudonymisation-techniques are encryption and hash function, which may be used alone or in combination with each other.\textsuperscript{99}

Encryption as a technique of pseudonymisation is often used in cloud computing.\textsuperscript{100}

With the use of encryption, personal data gets encrypted by replacing personal direct identifiers with codes, whereby those codes are kept within a secret list(key).\textsuperscript{101} The pseudonymised, key-coded data is then used to establish data security within the cloud computing process to protect the data against intruders.

This paper focuses not especially at encryption but rather at pseudonymisation in general to show the difference to anonymisation and the different regulations within the two European data protection frameworks.

Pseudonymisation can be done in two different ways: reversible (two way) pseudonymisation or irreversible (one way) pseudonymisation.\textsuperscript{102}

By replacing direct identifiers with numbers and deleting those lists of numbers(the key), pseudonymisation is conducted within one way, because there is “no way back” to replace the pseudonyms with the original identifiers. Such one way pseudonymisation may – depending on the robustness of the pseudonymisation-technique – render personal data to anonymous data and hence fall outside the scope of data protection rules.

With the use of reversible pseudonymisation, the identifiers are replaced by numbers/codes, but those pseudonyms are kept within a list in order to keep the possibility of re-identification. Hence reversible pseudonymised data constitutes always personal data for the key-holder, so that such data is not excluded from the scope of data protection rules. In situations where pseudonymised data is in the hand of a person other than the key-holder, the personal characteristic of such data may be changed. This situation will be discussed in the following sections as well as how the two frameworks provide incentives to implement pseudonymisation-techniques.

\begin{thebibliography}{99}
\bibitem{WP216} WP216, p.20f.
\bibitem{Hon/Millard/Walden} Hon/Millard/Walden, part 1,(2011), p.10f.,25,28; Spindler/Schmechel, JIPITEC(2/2016), p.169 rec.32; WP196, p.15; Esayas, EJLT Vol.6, No.2,(2015), p.9
\bibitem{WP136} WP136, p.18; WP216, p.29; WP196, p.15
\bibitem{WP136} WP136, p.18; WP216, p.29; WP196, p.15
\end{thebibliography}
4.1 Pseudonymisation under the DPD

Within the DPD, there is no Article or recital concerning pseudonymisation. Nevertheless this technique may be important under the current framework to ensure data security.

4.1.1 Pseudonymisation to render data anonymous?

Applying irreversible pseudonymisation, pseudonymised data may constitute anonymous data within the meaning of rec.26 DPD and may fall outside the scope of the Directive. Although the WP29 states within WP216, that “pseudonymisation when used alone will not result in an anonymous data-set”\textsuperscript{103}, it distinguishes within WP136 reversible from irreversible pseudonymisation with the consequence that one-way pseudonymisation (irreversible) “creates in general anonymised data”\textsuperscript{104}. Pseudonyms constitute indirect identifiers which may be combined together and linked to a person that one cannot say in general that one-way pseudonymised data is a form of anonymous data. In order to determine whether such data may be anonymous, the absolute-relative approach should be applied.

The more critical situation is when data has been pseudonymised with reversible pseudonymisation-techniques. It is indisputable that such data forms always personal data with regard to the key-holder. The problem lies in the case, where pseudonymised data is in the hands of a third party and the key is kept separately by the key-holder. Although the WP29 states in WP216 that pseudonymisation “will not result in an anonymous data-set”\textsuperscript{105}, it still shows that there may be cases, where pseudonymised data may not be personal data, but rather anonymised data.\textsuperscript{106} Following the absolute theory, this data is always personal also for the third party, because there is a key which is available by the key-holder.

Concerning the relative theory, pseudonymised data in the hands of a person other than the key-holder constitutes never personal data, because this person is not able to re-identify the data subject owing to the missing key.

As discussed above, both the WP29 and the CJEU use a modified theory, an absolute-relative approach,\textsuperscript{107} to determine data to be personal or anonymous.

\textsuperscript{103} WP216, p.20
\textsuperscript{104} WP136, p.18
\textsuperscript{105} WP216, p.20
\textsuperscript{106} “as, in the hands of the controller at least”, “not necessarily result in anonymisation”, WP216, p.29
\textsuperscript{107} See 2.1.2.3, 2.1.2.4
Using this approach, pseudonymised data may be personal to a third person who gains access to the key within an reasonable and appropriate effort. However a third person, who cannot get access to the key without excessive effort and when identification is not expected to take place, uses the pseudonymised data as anonymous data.\textsuperscript{108}

With the view of an absolute-relative approach, pseudonymisation may, in some situations, overlap with anonymisation.\textsuperscript{109}

\textbf{4.1.2 Pseudonymisation as security measure}

Applying reversible pseudonymisation, the key-holder as the controller is still processing personal data, that he still has to comply with all data protection rules of the DPD.

The question is then how to engage controllers to use pseudonymisation in order to grant data security.

According to WP29, pseudonymisation is not a method of anonymisation, but an useful security measure: although data remains personal, pseudonymisation reduces risks at stake for the individuals with regard to the processing of such data, which may lead to a more flexible application of data protection rules with less strict conditions, than in cases of processing direct identifiers.\textsuperscript{110}

Regarding the term “technical and organizational measures” in Art.17(1) DPD, pseudonymisation as well as anonymisation are technical measures: as security measures, the core security aspects are availability ensuring timely and reliable access to personal data, confidentiality including measures against unauthorized disclosure of and access to personal data and integrity ensuring authentic data not being maliciously or accidentally altered.\textsuperscript{111}

Pseudonymisation and anonymisation may significantly contribute to the integrity of the data in order to ensure that the data is not accidentally altered and to the confidentiality of the data to grant authorized disclosure of the data and to ensure for example secure communication or transmission of personal data.\textsuperscript{112}


\textsuperscript{109} Borges in Borges/Meents(2016), p.221, rec.33

\textsuperscript{110} WP216, p.20, WP136, p.18; Hon/Millard/Walden, part1,(2011), p.18

\textsuperscript{111} WP196, p.14ff.; Esayas, EJLT, Vol.6 No.2,(2015), p.18

\textsuperscript{112} WP196, p.15; Esayas, EJLT, Vol.6 No.2,(2015), p.18
The DPD provides only a few indirect incentives to use pseudonymisation.

Art.17(1) DPD concerning the security of processing mandates it only to the MS that controllers have to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing.

Rec.46 states the necessity to the MS to ensure that controllers must comply with appropriate technical and organizational measures regarding an appropriate level of security of processing.

Although the DPD with its legal nature of a Directive has to be transposed in national law, the Directive with its wording is not directly binding to the controllers.

This leads to the conclusion, that, although the WP29 and the literature emphasis pseudonymisation as an appropriate and useful security measure, the DPD does neither provide clear obligations or incentives to apply pseudonymisation nor does it contain clear benefits for those who use pseudonymisation such as an explicitly stated flexibility of the application of data protection rules concerning lawful processing.

Pseudonymisation may help to prove the compliance with data protection rules or to show the legitimate interest of the controller regarding fair and lawful processing, but looking at the huge amount of data processed, there needs to be more incentives and obligations to implement pseudonymisation to ensure a high level of data protection and an appropriate data and processing security.

4.1.3 Conclusion

Although the DPD is unfamiliar with the term of “pseudonymisation”, the literature and WP29 declare pseudonymisation to be an useful and appropriate security measure which in some cases may even lead to anonymous data.

The problem of pseudonymous data lies within the situations when pseudonymous data is processed by a third party not holding the key.

Following a modified theory, supplemented by the CJEU, the absolute-relative approach leads to the solution, that, depending on the actual effort to re-identify the individual, to get access to the key, in some cases, pseudonymised data constitutes anonymous data. Hence pseudonymisation overlaps with the term of anonymisation in such situations.

Regarding the key-holder, pseudonymous data is always personal data so that data protection rules of the DPD apply. To foster data protection and ensure a high level of data security,
pseudonymisation forms an appropriate and useful security measure which should be used by controllers in current times of big data and the Internet of things. Unfortunately, the DPD does not contain any obligation to use pseudonymisation and also does not provide incentives to the controllers to use pseudonymisation as an effective security measure.

It is therefore important to set incentives about the use of pseudonymisation to grant a high standard of data security which is not only in the interest of the individual to whom the data relates but also in the interest of the controller, to whom the data protection rules may be applied in a more flexible manner because of the reduction of risks.

4.2 Pseudonymisation under the GDPR

One novelty of the GDPR is the introduction of “pseudonymisation” within the new data protection framework.

The GDPR introduces pseudonymisation as a new category of data, which does neither directly identify the individual nor makes re-identification impossible. Pseudonymisation can therefore be seen as a third category of data next to personal data and its opposite anonymous data.\(^{113}\)

The GDPR recognizes the importance of pseudonymisation, so that it provides not only a clear definition of the term pseudonymisation but also several recitals and Articles concerning pseudonymisation as a perfect technical measure to ensure data security and secure processing.

According to Art.4(5) GDPR, “pseudonymisation 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”.

This definition should be read together with rec.26 GDPR, which states that “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”.

\(^{113}\) Bevott/Collins, PDP(2016,16(3)), p.13; Maldoff, The Privacy Advisor,(2016), p.2
Those provisions show that pseudonymisation constitutes an useful privacy-enhancing technique which removes direct identifiers by pseudonyms, that a data-set contains only indirect identifiable data. Pseudonyms as indirect identifiers are, regarding rec.26 GDPR, still personal data as they lead to possible identification of an individual, that pseudonymised data constitutes rather a sub-category than a third type of data.114 Although rec.28 GDPR explains that pseudonymisation can reduce the risks to the data subject concerned, pseudonymous data is, depending on the situation, not excluded from the scope of the GDPR.

4.2.1 Pseudonymisation to render data anonymous?
The GDPR states within rec.26, that generally pseudonymous data shall be considered to be personal data and hence within the scope of the data protection framework. But there might be situations, as under the DPD, where pseudonymisation may lead to render personal data not only pseudonymous but also anonymous. In the case of irreversible pseudonymisation, pseudonymisation is done within one-way in such a manner that the original personal data is not kept separately but rather is deleted. The definition of Art.4(5) GDPR requires the additional information to be kept separately and secured by technical and organizational measures. The wording should be read in a way that additional information means the original personal information which has been replaced by pseudonyms and is stored as a key as additional information. Therefore, irreversible pseudonymisation with no key containing the original data cannot be seen as pseudonymisation within the definition of Art.4(5) GDPR, that such pseudonymisation-technique may not only render personal data pseudonymous but also anonymous, that such data may fall outside the scope of the data protection rules. Hence not only under the DPD but also under the GDPR, irreversible pseudonymisation may be seen as an useful pseudonymisation-technique which may overlap with the term of anonymisation if the pseudonymous data constitutes effective anonymous data within the absolute-relative approach.

Also under the GDPR, the crucial situation is when a data-set of personal data has been pseudonymised with the use of reversible pseudonymisation and the pseudonymous data-set has been processed by a third person who is not holding the key.

114 Stevens, EDPL(2/2015), p.99
According to rec.26 GDPR, the pseudonymised data-set can still be attributed to a natural person with the use of the key, that such data-set should be generally regarded as information on an identifiable individual.

In order that other people than the authorized key-holder do not gain access to the key, the controller has to implement appropriate and effective measures. This obligation gives a first hint, that effectively secured pseudonymous data in the hands of a person other than the key holder may be anonymous for this person.

Furthermore, rec.26 GDPR talks about re-identification being “reasonably likely”, which shows that it always depends on the specific situation if data may be determined to be personal or anonymous.

Rec.26 s.2 GDPR “which could be attributed[…] by the use of additional information” should be read together with rec.26 s.3 and 4 GDPR, that this attribution needs to be “reasonably likely” taking into account “all the objective factors” of the specific situation.

Also in determining the data to be personal or anonymous, the GDPR uses an absolute-relative approach taking into account all the objective factors and measuring them to be likely reasonable to grant an reasonable appropriateness.

This approach in combination with the wording of rec.26 GDPR shows a flexibility within the Regulation concerning pseudonymous data.

In situations, in which the third party is not holding the key and it would be an excessive effort to get access to the key or other additional information, the attribution of the information to the individual by the third party is not reasonably likely. In those cases, the pseudonymised data, regarded from the point of view of the third party, may therefore be seen as effectively anonymous within the meaning of a “de-facto-anonymity”.

With regard to “all the objective factors” in rec.26 GDPR, there are three further relevant factors concerning the effective pseudonymisation using encryption. To determine encryption to be on an effective level, account should be taken to the strength of the encryption algorithm used, the length of the key and the level of security of the key-management to keep the key separate, secure and secret.

115 Rec.74,75 GDPR  
To assess the effective level of pseudonymisation, the development of the technology is also an important factor. Rec.26 GDPR states clearly, that not only the current state of technology should be taken in consideration, but also technological developments. This shows, that especially in situations of the usage of technological methods such as pseudonymisation and anonymisation, which are improving permanently because of on-going technical developments, the controller needs to use an technique on the basis of a prognosis regarding foreseeable future developments and to revise periodically the effectiveness-level of the technique used. So, with the use of effective pseudonyms, which create only an indirect association to the individual, and when the key is kept separately and secured, pseudonymous information may, depending on a case-by-case basis, appear to third parties other than the key-holder as anonymous data.\textsuperscript{117}

All in all, although rec.26 GDPR considers pseudonymised data to be personal as long as there is additional information kept separately and secure within a key, the pseudonymisation needs to be regarded within its effect towards the third party not holding the key.\textsuperscript{118} To grant an appropriate legal assessment, the characteristic of the specific data shall be determined from each point of view of the specific party concerned, with the consequence that the same pseudonymous data-set is personal for the key-holder but may be anonymous for a third party other than the key-holder. Hence, pseudonymisation may lead to render data anonymous depending on the special situation and depending on the view of the certain person concerned who is processing the pseudonymised data.

4.2.2 Lawful Pseudonymisation

According to the definition of “pseudonymisation” in Art.4(5) GDPR, the pseudonymisation process itself constitutes a form of “processing of personal data” within the meaning of Art.4(2) GDPR. With this definition of pseudonymisation, the GDPR states clearly that pseudonymisation itself means processing which has to be in argumentum e contrario in accordance with the provisions and obligations of the data protection framework.

\textsuperscript{117} Karg, DuD(8/2015), p.524
\textsuperscript{118} Karg, DuD(8/2015), p.524
As mentioned above, within the current legal framework, the DPD, there are discussions about the processing-characteristic of anonymisation and also of pseudonymisation because of the lack of legal certainty and definitions within the DPD. Following the opinion, that techniques such as anonymisation and pseudonymisation do not perform “processing” within the meaning of the DPD, those techniques also do not have to comply with the provisions of the Directive, hence they do not have to be lawful and in accordance with the data protection principles. This opinion causes a massive lack of data protection: although anonymisation and pseudonymisation might be effective data security measures, they may be carried out with purposes not compatible with the data protection framework.

By defining pseudonymisation as a form of processing, the GDPR creates certainty about the discussion if anonymisation and, as another data security method, pseudonymisation constitute processing within the meaning of the framework. The Regulation goes one step further to effective data protection with explicitly defining pseudonymisation as a form of processing within not only the recitals but within Art.4(5) GDPR. Hence, the pseudonymisation process itself has to be lawful and in accordance to the data protection principles of the GDPR – irrespective of the outcome of the pseudonymisation concerning personal or anonymous data.

First, pseudonymisation as further processing, might be lawful, if the purpose of the pseudonymisation process is compatible with the initial purpose according to Art.5(1)(b), rec.50 GDPR. To assess the compatibility of the further processing, account needs to be taken to the “compatibility test” within Art.6(4) GDPR.

If the purpose is not compatible with the initial one, the pseudonymisation process might still be lawful under the condition of Art.6(1)(c) or Art.6(1)(f) GDPR.

It is not only in the interest of the controller to use pseudonymisation in order to ensure data security and secure data processing, but also in the interest of the individual, that the processing of its data is not only lawful under the GDPR but also secured within a technical manner. This leads to the conclusion, that Art.6(1)(f) GDPR, the lawful processing in the interest of the controller which is not overridden by the data subject's interest, is in most cases of pseudonymisation fulfilled, that the pseudonymisation process is lawful under the GDPR.
Furthermore, the GDPR contains several obligations to the controller to implement technical security measures with explicitly referring to pseudonymisation. For example to comply with the obligation to establish data protection by design, the controller shall implement “appropriate technical[…] measures, such as pseudonymisation”\textsuperscript{119} and Art.32(1)(a) GDPR names directly pseudonymisation as an appropriate tool to comply with the obligation of secure processing. Using pseudonymisation to fulfill those obligations, the pseudonymisation process may therefore be also lawful under Art.6(1)(c) GDPR.

So with the definition in Art.4(5) GDPR by describing pseudonymisation as a form of processing, the Regulation states clearly that pseudonymisation itself has to be lawful and in accordance with the data protection principles, which may be fulfilled as “further processing” under Art.5(1)(b), rec.50 GDPR or as lawful processing under Art.6(1)(c) or (f) GDPR.

4.2.3 Pseudonymisation as security measure
The novelty about pseudonymisation within the GDPR is not only that it is mentioned and explained within a definition, but that its important usefulness for securing data in a time of ongoing technical development is also acknowledged by several obligations and incentives under the GDPR to implement pseudonymisation as a technical security measure. In today's world of the on-going technological development and the constant growth of processing a huge amount of data, it is important to note, that data processing shall be legitimate and lawful under the legal framework but lawful processing needs also to be ensured in a technical way to provide secure processing and secure data which shall be technically protected against any intruders.

The GDPR contains therefore many provisions about pseudonymisation which can be roughly divided into the two categories of “obligations” and “incentives”.

4.2.3.1 Obligations
With the new introduction of Privacy by Design and Privacy by Default, Art.25(1) GDPR contains also an obligation to the controller to implement technical and organizational measures, such as pseudonymisation. Data Protection by Design/Default “means that privacy should be a feature of the development of a product, rather than something that is tacked on
Pseudonymisation is therefore seen as an appropriate technical measure to implement and comply with the data protection principles, such as the data minimization principle of Art.5(1)(c) GDPR.

Another obligation is included in Art.32(1)(a) regarding the security of processing: the controller as well as the processor “shall implement appropriate technical and organizational [security] measures”, whereby pseudonymisation is listed to be appropriate. Hence, controllers and processors have the obligation to implement pseudonymisation as a technical security measure concerning secure processing.

In order to grant an effective exception to the purpose limitation principle for data processing for scientific, historical and statistical research, such processing shall be subject to safeguards such as appropriate technical and organizational measures to ensure the data protection principles, especially the principle of data minimization, whereby pseudonymisation is particularly mentioned as such measure.

4.2.3.2 Incentives
Pseudonymisation as an effective tool to reduce the risks to data subjects, is so important in the current time of technical development, that controllers should not only implement pseudonymisation because of an obligation, but they should rather use pseudonymisation in all situations to grant effective and secure data protection. To encourage controllers and processors to pseudonymise data-sets, there need to be incentives which may provide advantages to those who use pseudonymisation. This goal to “create incentives to apply pseudonymisation” is recognized by the Regulation and set down in rec.29 GDPR.

As already mentioned in some obligations, it is a general incentive to use pseudonymisation to show compliance with the data protection principles, especially with the principle of data minimization of Art.5(1)(c) GDPR.

Solely the replacing of an direct identifier as a name by an indirect identifier as a pseudonym may constitute already an appropriate measure to ensure data minimization. It is therefore generally in the interest of and an advantage for the controller to use pseudonymisation to show compliance with the Regulation.

---

120 Maldoff, The Privacy Advisor,(2016), p.3
121 Art.5(1)(b) GDPR
122 Rec.156,Art.89(1) GDPR
123 Rec.78 GDPR
Pseudonymisation may also be implemented to “enable” further processing: if further processing is compatible with the initial purpose, account shall be taken to the “compatibility test” in Art.6(4) GDPR. Within this test, the usage of pseudonymisation represents an important factor to ascertain the compatibility with the initial purpose.

Another incentive may be seen in Art.33(1) GDPR: in cases of personal data breach, the controller shall notify the supervisory authority, “unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.” This exception shows that the use of pseudonymisation may lead to a flexible applicability of data protection rules. Pseudonymisation reduces the risks to the data subject (rec.28 GDPR), that – depending on the effectiveness of the pseudonymisation-technique – the data breach does not result in high risks with the consequence, that the exception of Art.33(1) is fulfilled. Hence, although the pseudonymisation is not demanded by this provision, its usage is useful to benefit from the exception, which directly sets an incentive to implement such technique.

Also in the situation of personal data breaches resulting in high risks, the controller is usually obliged to communicate the data breach to the data subject (Art.34(1) GDPR). Article 34(2) (a) GDPR contains an direct incentive, by particularly stating encryption as a form of pseudonymisation as a possible condition to fulfill the exception with the benefit, that the communication to the data subject is no longer required.

Furthermore, in cases of data protection impact assessments prior to the processing, the use of pseudonymisation constitutes an important factor to show the minimizing of possible risks and the compliance with the Regulation, Art.35(7)(d), rec.90 GDPR.

A provision which also shows a flexible applicability of the data protection rules is Art.11(2) GDPR. According to this Article, Art.15-20 shall not apply in cases, in which the controller is able to demonstrate that is is not in a position to identify the data subject. Hence, “consistent with the approach to pseudonymisation on data breach issues, the GDPR appears to relax disclosure requirements”\textsuperscript{124} in situations, in which data has been pseudonymised.

\textsuperscript{124} Lee/Breslaw, Delphix,(2016), p.7
This exception in Art. 11(2) GDPR forms a great flexibility of data protection rules to the benefits of the controller: to ensure all rights granted to the individual by Art. 15-20 GDPR or to not have to take into consideration of those rights is a big difference for the controller concerned regarding the amount of work, time and effort to grant the data subject's rights.

Although this paper is focusing on pseudonymisation in general, regard should be taken to the fact, that some of the incentives explicitly name “encryption” next to pseudonymisation. Within the “compatibility-test” of Art. 6(4)(e) GDPR, appropriate safeguards, “which may include encryption or pseudonymisation” shall be taken into account. Art. 32(1)(a) GDPR, lists “pseudonymisation and encryption of personal data” as appropriate security safeguards concerning secure processing. As examined above, encryption constitutes a technique of pseudonymisation, that the wording of the two provisions above could be misleading

The conceptual differentiation of the two terms does however not stand in contrast with the fact that encryption as a special technique is included in the generic term of pseudonymisation. With the special naming of encryption in the GDPR, the Regulation rather acknowledges the particular status of encryption in comparison with other pseudonymisation-techniques, what can be supported by the wording of rec.83 and Art.32(3)(a) GDPR, which also emphasize encryption as an appropriate technical security measure.125

4.2.3.3 Quality of Pseudonymisation

Problems may occur because of the formulation of “appropriate” safeguards or technical measures. The GDPR always uses the term “appropriate” when talking about the quality of the security measure, but there is no provision defining the term “appropriate” or measuring the necessary quality of the security measure.

Art.32(2) GDPR contains further guidance about determining an appropriate level of security, but still, it does not define the term of appropriate safeguards.

Because the GDPR is formulated in a technological-neutral manner to apply its provisions to several cases independent on the technique used and to prevent circumvention,126 Art.40 GDPR leaves the opportunity to further clarify indefinite terms or provisions within codes of conduct. With the purpose to specify the application of the Regulation, codes of conduct may also be set up with regard to the pseudonymisation of personal data, Art.40(2)(d) GDPR.

125 Marnau, DuD(7/2016), p.431

126 Rec.15 GDPR
4.2.3.4 Conclusion

With the inclusion of pseudonymisation in the GDPR, with requiring controllers and processors to implement this technique to comply with the data protection principles and with several incentives to use this technique, the new data protection framework recognizes pseudonymisation as an important tool and effective technical measure to ensure data security and secure processing.

Pseudonymisation is thus not only in the interest of the controller but also in the interest of the individual what makes the usage thereof even more important.

To encourage the controllers to implement such techniques, the GDPR sets a goal to create incentives to use pseudonymisation even in those cases, in which there is no pseudonymisation demanded by the Regulation. This goal is already achieved by providing several provisions which grant flexible applicability of data protection rules what results in benefits and therefore in incentives for the controller to implement and use pseudonymisation.

4.2.4 Conclusion

With the introduction of “pseudonymisation” within the new legal framework, the GDPR acknowledges the high importance of pseudonymisation in order to grant effective data protection.

The Regulation mentions not only pseudonymisation within the recitals but also provides a definition and several Articles concerning pseudonymisation as an useful data security measure.

Regarding the problem if pseudonymisation may lead to anonymous data, the GDPR provides with its definition in Art.4(5) GDPR and rec.26 GDPR guidance so that in some cases pseudonymised data, although generally assumed as personal data\(^\text{127}\), may considered to be anonymous data depending on a case-by-case basis taking into account the “reasonably-likely-test” under the absolute-relative approach.

Furthermore, the GDPR provides guidance by clearly defining pseudonymisation as a form of processing within Art.4(5) GDPR and in argumentum e contrario thereof, that the pseudonymisation-technique itself has to be lawful under the GDPR, independent of the outcome of the pseudonymisation process.

\(^\text{127}\) Rec.26 GDPR
Although the facts, that with the use of pseudonymisation the data remains, at least for the
key-holder, personal and that the pseudonymisation-technique has to be lawful and in accord-
ance with the data protection principles of the GDPR, may discourage controllers and pro-
cessors to implement pseudonymisation, the Regulation counteracts this possible consequence
by providing obligations and several incentives to use pseudonymisation as a proper data se-
curity measure.

The GDPR acknowledges the high importance of pseudonymisation as a security measure to
ensure not only lawful processing but also technical secure processing and the security of
data. With the creation of several incentives, the GDPR grants benefits in form of flexible ap-
lication of data protection rules to those who use pseudonymisation.

4.3 Conclusion – Comparison of Pseudonymisation under DPD & GDPR

The DPD does not mention pseudonymisation at all. There is no definition or any provision
about the use of pseudonymisation.

But, although the DPD does not contain the term “pseudonymisation”, the pseudonymisa-
tion-technique is discussed as a useful data security tool by the literature and the WP29 re-
garding the provisions of the DPD.

The WP29 emphasizes clearly, that pseudonymisation is not a method of anonymisation but
rather an appropriate security measure reducing the risks to the individual and ensuring there-
fore a proper level of data security.

Problems occur, similar to the problem of anonymisation, in assessing if the pseudonymisa-
tion process itself needs to be lawful under the DPD and if pseudonymisation may render per-
sonal data anonymous.

There are opinions talking about pseudonymisation as a form of further processing which
needs to be in accordance with the DPD, but there are also points of view which focus on the
controller, that declaring pseudonymisation as further processing would discourage the con-
trollers to implement pseudonymisation-techniques and that pseudonymisation with the pur-
pose to reduce the risks of the individual and the aim to ensure data security shall not need to
be lawful and in accordance with the data protection principles.

With introducing a definition and several provisions about pseudonymisation, the GDPR
brings, to a certain degree, those discussions to an end and provides thereby legal certainty.
Not the pseudonymisation-technique as such is one novelty within the GDPR, but the introduction of this technique within a legal framework and the recognition of it as an useful security measure.

In opposite to the DPD, the GDPR clearly defines “pseudonymisation” and contains several provisions talking about the technique itself and the need to implement pseudonymisation. Although the problem if pseudonymisation may lead to anonymous data remains, the GDPR provides firstly a general assumption that pseudonymised data in general remains personal data. But reading this provision in combination with the other sentences of rec.26 and in accordance with the definition of Art.4(5) GDPR, the GDPR provides guidance, that the re-identification needs to be reasonably likely taking into account all the objective factors that pseudonymisation may render personal data anonymous depending on the GDPR's absolute-relative approach and on a case-by-case basis.

Regarding the discussion about lawful pseudonymisation-process, the GDPR states clearly in Art.4(5) that pseudonymisation constitutes a form of processing which in argumentum e contrario needs to be lawful and in accordance with the data protection principles. With this provision, the GDPR seizes on the previous discussions in the literature, provides proper guidance and ensures a high level of protection by demanding every pseudonymisation-process to be lawful.

Looking at obligations and incentives about pseudonymisation, the DPD does not contain any provisions regarding the importance of pseudonymisation as a security measure. Although the WP29 and the literature declare pseudonymisation as an appropriate security measure granting data security and secure processing, the DPD does neither mandate any obligation to implement this technique nor does it provide any direct incentives to the controller.

With Art.17(1) DPD, the Directive only contains an indirect obligation/ incentive to the controller with an obligation to the MS to ensure the implementation of technical safeguards. The only direct incentive to the controller to implement pseudonymisation under the DPD is to demonstrate the willingness to reduce risks and ensure compliance with the data protection rules.
Regarding obligations and incentives about pseudonymisation, there is the actual important shift and novelty of the GDPR. The GDPR recognizes the high importance of pseudonymisation as an useful security measure by setting clear obligations to implement this technique and by providing several incentives for using pseudonymisation. Especially the provisions containing incentives are very important to encourage controllers/processors to actually implement pseudonymisation-techniques to grant not only data protection and data security within a legal manner but also within a technical manner against any intruders. With the incentives in the GDPR, the controller who uses pseudonymisation as a security measure may easily demonstrate compliance with the data protection rules and may benefit because of a flexible applicability of data protection rules in cases of lawful pseudonymisation. Hence, by not only introducing a definition of “pseudonymisation” but also by providing guidance about the pseudonymisation-technique itself and by setting obligations and incentives to implement pseudonymisation, the GDPR recognizes the importance of pseudonymisation as an useful security measure which shall be used in the interest of the controllers/processors and in the interest of the individuals concerned to grant proper data protection in a legitimate and a technical manner.

All in all, by comparing the DPD to the GDPR, the latter goes one step further into the direction of proper data protection with firstly acknowledging pseudonymisation as an important data security measure in times of big data and the internet of things, secondly with providing guidance and legal certainty about the implementation of this technique and its consequences and thirdly with containing several obligations and incentives which grant benefits and flexible applicability of data protection rules.
5. Practical Impact of the GDPR for Cloud Computing

The cloud computing process in general consists of uploading, transferring, combining, storing personal data with the consequence that there is always a form of processing within the meaning of data protection rules. Especially in cases of SaaS, when personal data has to be outsourced to the online platform of the cloud provider, attention needs to be drawn to grant data protection and data security.

To know if data protection rules apply, the cloud user and cloud provider need to determine the characteristic of the data concerned. Only the category of personal data falls within the scope of the GDPR.

To determine data to be personal or anonymous, the GDPR provides proper guidance in using an absolute-relative approach by taking into account all the means reasonably likely and all objective factors on a case-by-case-basis.

In assessing the usefulness of anonymisation and pseudonymisation, different cloud computing scenarios need to be distinguished.

When a company uses its own private cloud, the company itself acts as cloud user and cloud provider at the same time and as the data controller within the meaning of Art.4(7) GDPR.129

When a public cloud is used, usually the roles of cloud user/cloud provider and controller/processor fall apart. Providing a public cloud, the cloud provider offers its cloud service to a wide range of cloud users. When a cloud user then uploads and outsources his data to the cloud, he is the one who determines the ultimate purposes of the processing and decides on the outsourcing and the delegation to an external organization. Therefore, usually in cases of public cloud computing, the cloud user acts as a data controller(Art.4(7) GDPR) and the cloud provider on behalf of the user as a data processor according to Art.4(8) GDPR.130

There might be also situations, in which the cloud provider processes the uploaded data for its own purposes that such cloud provider act not longer as a data processor but rather as a joint controller or a controller within the meaning of Art.4(7) GDPR.

129 Borges/Brennscheidt in Borges/Schwenk(2012), Chap.3, p.58
130 WP196, p.7ff.; Borges/Brennscheidt in Borges/Schwenk(2012), Chap.3, p.58
For this recommendation, the focus shall be on the usual situation of a public cloud, that the cloud user acts as a data controller and the cloud provider as a data processor.

Although the GDPR still distinguishes between data controller and data processor within the definition and in regard to different obligations, the role of data processors has been brought mostly into line with the role of data controllers.\textsuperscript{131,132}
Therefore, it is even more important to determine the usefulness of anonymisation and pseudonymisation for cloud computing services to grant data protection and security and to comply with the rules of the GDPR.

\subsection*{5.1 Anonymisation}
Anonymisation as a technique to render personal data anonymous seems at the first impression as a useful mechanisms to exclude the whole cloud computing process from the scope of the data protection framework.
The cloud user could prior to outsourcing the data to the cloud anonymise the personal data, with the consequence that, depending on the robustness of the anonymisation-technique used, anonymous data would be processed.

The problem of anonymisation in such scenarios is that the data is rendered anonymous in a way that re-identification is reasonably likely no longer possible. This consequence is usually not in the interest of a cloud user: the cloud user outsources mostly the data to the cloud with the purpose that he can use the data again all the time and independent of his current location.
It is therefore important for the cloud user, that he has access to the original data that he effectively can use the data for his purposes, which would be not longer granted if the original data would be effectively anonymised prior to the outsourcing.\textsuperscript{133}

The same problem occurs, if the outsourced data of the cloud user gets anonymised by the cloud provider. Again, the consequence of effective anonymisation is that the original data is

\textsuperscript{131} Art.82 GDPR: the processor as well as the controller have to compensate the data subject for suffered damage as a result of an infringement of the Regulation and the processor – next to the controller – shall also be held liable for the entire damage. The processor shall also be subject to administrative fines and additional penalties in cases of an infringement of the Regulation,Art.82,84 GDPR. The data subject also shall have the right to an effective judicial remedy against a controller as well as a processor, Art.79 GDPR.
\textsuperscript{132} McKean, Olswang EU Data Protection Reform, p.11
\textsuperscript{133} Hennrich, Cloud Computing(2016), p.135
deleted in a way that all direct and indirect identifiers are eliminated, which is not in the interest of a cloud user, who stores his data in a cloud for the purpose to have access to the original data.\textsuperscript{134}

One situation in which anonymisation may be a reasonable solution, would be, when the cloud provider wants to further process the user's data for a purpose not compatible with the initial purpose.

Another situation would be, when the cloud user is not or no longer interested in the original data but wants still to process the data for statistical or research purposes. Then it seems to be the best way to effectively anonymise the original data with the consequence that the further processing of anonymous data does no longer fall under the scope of the GDPR.

But to effectively anonymise personal data, both the cloud user and the cloud provider have to bear in mind that the GDPR requires the anonymisation process itself to be lawful and an appropriate level of effective anonymisation within an absolute-relative approach thereby taking into account not only the current state of technology but also possible future developments with the obligation to constantly revise the anonymisation-technique used.

So if the original data is not or no longer needed, anonymisation-techniques could provide benefits to the cloud provider, the cloud user and to the individual to whom the information relates. Cloud user and cloud provider would no longer process personal data, the interest of the individual to protect its privacy would be granted and the people's confidence in cloud computing would be established.

5.2 Pseudonymisation

Pseudonymisation would be the proper technical solution in cloud computing with reducing the risks of re-identification and unauthorized access, but nonetheless keeping the data's utility.\textsuperscript{135}

Both the cloud user and the cloud provider need to ensure data protection and data security. Pseudonymisation could be done prior to the outsourcing of the data to the cloud. Depending on the robustness of the pseudonymisation-technique used and on an effective key-management, the cloud user would still process personal data with the consequence that he as the key-

\textsuperscript{134} Kian, Cloud Computing(2016), p.153

\textsuperscript{135} Rabe/Wagner, DuD(7/2016), p.437; Maldoff, The Privacy Advisor,(2016), p.2
holder always has access to the original data. Also the cloud provider could benefit from this method: ensuring, that gaining access to the key would constitute an unreasonable high effort to the cloud provider, the pseudonymised data outsourced to the cloud would be anonymous data from the point of view of the cloud provider, that a cloud provider could process the pseudonymised data of the user without being in compliance with the rules of the GDPR. Hence, the processing of pseudonymised data by the cloud provider would be outside the scope of the data protection rules.

In typical concerns about lack of control and lack of information in cloud computing processes, it is the best solution to provide cloud computing services with an pseudonymisation method prior to the outsourcing of the data. This method grants the cloud user as the key-holder the control over the original data and the compliance with data protection principles and the cloud provider may, depending on a case-by-case basis, processes the pseudonymised data as anonymous data without having any regard to the GDPR.

Especially in having regard to ensure data minimization, the cloud user as a controller is obliged by Art.25(1),(2) GDPR to implement pseudonymisation as a method of Data Protection by Design/ by Default.

When the cloud user as the data controller pseudonymises the data prior to uploading data to the cloud, the user ensures, that only him as the original data controller is able to use the personal data and not the cloud provider or other third parties.

But also in other situations, when pseudonymised data does not constitutes anonymous data from the point of view of the cloud provider, pseudonymisation as a security measure is still necessary.

The main characteristic of cloud computing is that the capacity of the servers can be used until optimum capacity in a way that data is stored at different servers all over the world. This method of storing data at different servers requires effective data security and secure processing to protect the data against any intruders, damages, unauthorized access or even data loss.

Because of high risks of unauthorized access and data loss in cloud computing, the implementation of pseudonymisation is mandated by Art.32(1)(a) GDPR to the controller and the

---

136 Hon/Millard/Walden, Part1,(2011), p.25,28
137 Spindler/Schmechel in JIPITEC(2/2016), p.169 rec.32
processor. Hence the controller and the processor need to make sure, that effective pseudonymisation is implemented in the cloud computing process. Furthermore, both the cloud user and the cloud provider benefit from the usage of pseudonymisation under the GDPR, because both may easily demonstrate the compliance with the Regulation what may result in a flexible applicability of the data protection rules. Although the personal data remains personal to both, cloud user and cloud provider will have the advantages of a less strict application of the GDPR because of implementing effective pseudonymisation as a security measure.

Another major impact of pseudonymisation from the point of view of the cloud provider is to gain the confidence of users in cloud computing with the consequence of increasing clients. Already under the DPD, processors have the duty to ensure confidentiality and to adopt security measures under Art.17(2) DPD and the controller shall choose only such processor who uses technical security measures, Art.17(1) DPD. The same obligation remains under Art.28(1) GDPR, what shows, that the usage of pseudonymisation as security measure is not only in the interest of the cloud provider to gain the users confidence but that it is also an important criterion under the obligation on the cloud user to choose a trustful cloud provider.

In order to assure the implementation of pseudonymisation, the cloud provider should contain in the contract with the cloud user clauses with sufficient guarantees about the usage of pseudonymisation as a technical security measure. Furthermore, cloud provider using pseudonymisation should be certified as trusted clouds by independent certification bodies according to Art.42, 43 GDPR.138 Such certification would be in the interest of both: the cloud provider would benefit by proving confidentiality to the users and the cloud user could easily choose an appropriate processor within his obligation under Art.28(1) GDPR.

In conclusion, both the cloud user as data controller and the cloud provider as data processor only benefit from the implementation of pseudonymisation as an useful privacy-enhancing technique what protects the data to a higher degree.

---

Ensuring a lawful pseudonymisation process and an effective level of pseudonymisation, both can meet the security obligations of the GDPR and show in addition easily the compliance with the data protection rules what leads to a flexible applicability of the Regulation.

6. Final Conclusion

In current times of on-going technological developments, a parallel online-world in the Internet, Big Data and the Internet of Things, concerns have arisen if data protection can still be given at all. In the example of cloud computing, the tension between technological, online services and data protection has come to a head in the sense of “data protection vs. cloud computing?”.

Not only in the interest of the individuals concerned, but also of the cloud user and of the cloud provider, there is a need to establish legal certainty about the applicability of data protection rules to cloud computing and how to comply with such rules in an effective manner. Under both legal frameworks, the key-factor to determine the applicability of data protection rules to cloud computing is “personal data”. Although under the current framework of the DPD, there are several opinions about the examination of personal data, the WP29 and the CJEU provide guidance in an appropriate way using a “middle-way”, an absolute-relative approach.

This approach is included within the new framework the GDPR looking at all the means reasonably likely and all the objective factors on a case-by-case basis.

To exclude the whole cloud computing process from the scope of data protection rules, the original data needs to be anonymised in an effective way ensuring under both legal frameworks lawful anonymisation processing as further processing and an appropriate level of anonymisation within an absolute-relative approach taking into account not only the current state of technology but also future technological developments.

In most situations, in which personal data has not been rendered anonymous, the question about “data protection vs. cloud computing” remains.

Cloud computing with its characteristic of storing data on several severs all over the world is susceptible to unauthorized access, damages or even data loss.
To grant not only data protection in a legal manner but also in a technical way, the implementation of technical security measures, especially pseudonymisation, becomes more and more important.

Although pseudonymisation has been discussed in the literature under the DPD, the new Regulation introduces pseudonymisation within the definitions and provides obligations and several incentives about the usage thereof what creates a serious novelty within the GDPR.

Even though pseudonymisation may in some cases render personal data anonymous and exclude the scope of data protection rules, pseudonymisation is particularly recognized as an useful security measure.

The GDPR increases the value of pseudonymisation with the acknowledgment of it as an appropriate, useful security measure and shows a current need to implement pseudonymisation to every processing in order to grant data security, secure processing and hence a higher level of data protection.

Therefore, the GDPR provides a proper guidance about personal data, anonymisation and notably pseudonymisation, and ensures an important change and one step further to effective data protection.

So with the use of pseudonymisation as an effective data security tool, even cloud computing with its high risks for data security and data protection can be carried out in accordance with data protection rules with the consequence that, especially under the GDPR with its proper guidance, there will be no longer the tension in the sense of “data protection vs. cloud computing”.
## Table of References

### Judgments/Decisions

- Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, Judgment of the Court (Second Chamber) of 19 October 2016

- Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, Opinion of Advocate General Campos Sánchez-Bordona delivered on 12 May 2016


### Treaties/Statutes/Opinions

- 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 (DPD), OJ No L 281/31-50

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L 119/1-88

- *Commission of the European Communities*, COM(90) 314 final, Brussels, 13 September 1990, Commission Communication on the protection of individuals in relation to the processing of personal data in the Community and information security

- *Commission of the European Communities*, COM(92) 422 final, Brussels, 15 October 1992, Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, 10 April 2014


Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, WP196, 1 July 2012

Books, Articles and Recommendations

Bevitt, Ann/ Collins, Amy, Seven key data protection New Year's resolutions companies should be making, in Privacy & Data Protection (PDP), 2016, 16(3), pp. 13-15


Brimsted, Kate, Anonymisation – a process living on borrowed time?, in Privacy & Data Protection (PDP), 2014, 14(7), pp. 3-5

Burton, Cédric/ Hoffman, Sára, Personal Data, Anonymization, and Pseudonymization in the EU, in The WSGR Data Advisor, 15 September 2015

Data Protection Commissioner (DPC) Ireland, Anonymisation and Pseudonymisation, online available: https://dataprotection.ie/viewdoc.asp?DocID=1594&ad=1


- Esayas, Samson Yoseph, The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the „all or nothing“ approach, in European Journal of Law and Technology (EJLT) Vol.6 No.2 (2015)


- Härting, Niko, Anonymität und Pseudonymität im Datenschutzrecht, in NJW 2013, pp. 2065-2071


- Herbst, Tobias, Was sind personenbezogene Daten?, in NVwZ 2016, pp. 902-906

- Hon, W Kuan/ Hörnle, Julia/ Millard, Christopher, Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3, 9 February 2012, Queen Mary University of London, School of Law, Legal Studies Research Paper No 84/2011

Hullen, Nils, Entwürfe der Eu Datenschutz-Grundverordnung im Überblick – Pseudonymisierung, Privacy-by-Design und Ko-Regulierung, in jurisPR-ITR 19/2015 rec.2


Karg, Moritz, Anonymität, Pseudonyme und Personenbezug revisited?, in Datenschutz und Datensicherheit (DuD) Vol.39, Issue 8 2015, pp. 520-526


Maldoff, Gabe, Top 10 oprational impacts of the GDPR: Part 8 – Pseudonymization, in The Privacy Advisor, Westion Research Center, 12 February 2016, online available:


- McKeen, Ross, EU Data Protection Reform: Where are we – and what can you do to prepare?, Olswang, online available: http://www.olswang.com/media/48316310/olswang_s_top_12__eu_data_protection_reform.pdf


- Oswald, Marion, Data anonymisation and managing risk – the ICO's new code, in Privacy and Data Protection (PDP), 2012, 13(2), pp. 3-6


Schaar, Katrin, DS-GVO: Geänderte Vorgaben für die Wissenschaft – Was sind die neuen Rahmenbedingungen und welche Fragen bleiben offen?, in ZD 2016, pp. 224-226


Treacy, Bridget, Expert comment, in Privacy & Data Protection (PDP) 2012, 13(2), p.2

von dem Busche, Axel/ Stamm, Markus, Data Protection in Germany, C.H. Beck München 2013

Welfare, Damien, Clarifying the scope of personal data, in Privacy & Data Protection (PDP) 2012, 12(7), pp. 7-10

Web Links