UiO : Faculty of Law
University of Oslo

The Relations of Controllers, Processors and Sub-processors under the DPD and GDPR

First Deliberations: Does the GDPR represent progress in the digital age?

Candidate Number: 8016

Submission Deadline: [01/12/2016]

Number of words: 17.972[18.000]

Table of Contents

Abbreviations:

Art.	Article
BDSG	Bundesdatenschutzgesetz
CJEU	Court of Justice of the European Union
DPD	Data Protection Directive (The Directive 95/46/EC of 24.10.1995)
ECJ	European Court of Justice
e.g.	for example
EU	European Union
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679 of 27.4.2016)
No.	Number
p.	Page
rec.	Recital
Vol.	Volume
WP	Art.29 Working Party

1 Introduction

The digital age or information age constitutes one of the three big periods in human history after the agrarian society and the machine age. The digital age manly roots in the development of the internet.

One of the most recent manifestations of the internet is the increase use of cloud-computing. Like all new technologies embodies also cloud-computing risks. One of the basic problems with cloud-computing is that the cloud user does not use the computing power on his own computer but from a third person. This means that data must be processed between those parties.

The main risks of cloud-computing stem from the relation of the parties involved[1] and the act of processing data. Those risks fall in the scope of data protection law.

In the EU are two main sets of law which regulate data protection the Data Protection Directive[2] and the upcoming General Data Protection Regulation[3]. In particular the construct of cloud-computing pushes the current DPD to the limit.

This leads to the question if the GDPR fulfills the expectations to meet the requirements of the the future and with that represents progress in the digital age.

To asses the question if the GDPR can satisfyingly regulate on the field of the relation between the parties in cloud-computing and if it can mitigate the risk for individuals will first cloud computing be defined and the service and rollout models be shown. Afterwards will the definitions of: processing, controller, processor and sub-processors under both texts of law be compared, as well will be determined who actually is controller in the majority of cloud-computing cases.

Before getting to the core of the thesis will the relations in cloud computing between controller and processor and processor and sub-processor under both regulatory frameworks be shown. Therefore will first the contractual requirements be shown, the rights of selection and control, the decisional authority and the allocation of responsibility. Afterward will be compared and concluded.

In the core of this master thesis will the relation of controller and sub-processors be compared under both sets of law. This relation is highly controversial under the current DPD and is

[1] Namly: Controller, processor and sub-processor.

[2] 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.

[3] 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).

going to cause major legal uncertainties, because of the reasons shown above, on the field of cloud-computing when the GDPR enters into force.

For this will the right execution models under the DPD be shown and discussed and than in an own analysis transferred to the GDPR. Afterwards will be concluded with an own opinion.

In the conclusion will be quickly summaries and the question will be answered if the GDPR represents progress in the digital age.

1.1 Methodology

This thesis shall not be a full analysis of cloud-computing. Cloud-computing is used as an example for the practical relevance of the topic.

For this master thesis I did mostly use articles and court decisions from Europe, law internet blogs and the law itself.

Because of the worldwide good reputation of german legislation and jurisdiction on the field of data protection law I focused especially on german literature.

Data Protection Law has in Germany a long history, the first Data Protection law was the hessian data protection Law, which entered into force 1970. So that a vast amount of literature exists on the topic.

For the research did I also focus on english literature, especially the texts of official EU bodies like the Art.29 Working Party.

The arguments in discussions in this paper are strongly based on the wording of the law.

The conclusion of this thesis must be seen in the light of the literature being used.

1.2 Defining cloud-computing

There is no common definition on what cloud-computing is. Cloud-computing is a developed out of grid-computing. This development brings new risks and needs for new regulation but also allows to transfer legal thoughts from the primal model.[4]

[4] Hamdaqa/Tahvildari, Cloud Computing Uncovered: A Research Landscape, in Advances in Computers(2012),vol.86,p.41-85(79ff.).

Grid-computing can be seen as the ancestor of the cloud it describes the bundling of computing power all over the world to work together on one task.[5] This is mostly done for big scientific experiments.

Grid-computing is a reversed form of cloud-computing. In cases of cloud-computing do several clients use one provider together, but not to achieve one common purpose.

The European Commission defines Cloud-computing as the storing, processing and use of data on remotely located computers accessed over the internet.[6]

Whereas the literature defines it as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[7]

The definitions seem to very strongly but are in essence the same.

In the context of this articles cloud computing will consequently be defined as: a complex structure, enabled by the internet, and whereas services are provided for the end-user, also the end-user is empowered to implement the majority of actions in quite simple and convenient environment.[8]

There are three groups of cloud-services: IaaS, PaaS and SaaS and the different rollout models of those services: public cloud, private cloud and hybrid cloud.[9]

Cloud computing comes with the major advantages of: Flexibility, to scale needed computing power as needed within minutes.

Security, lost hardware do not necessarily mean a data loss, because of backups and encryption.

Cost efficiency, because the infrastructure is shared by many and soft- and hardware must not be bought and can be optimized across the network.

---

5 Honbo, The Internet of Things in the Cloud: A Middelware Perspective,(2012), p.260.

6 Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me?, Memo of the European Commission,(27.09.2012).

7 Stitilis/Malinauskaite, Compliance with basic principles of data protection in cloud computing: the aspect of contractual relations with end-users, in European Journal of Law and Technology, vol.5, nbr.1,(2014).

8 Stitilis/Malinauskaite, Compliance with basic principles of data protection in cloud computing: the aspect of contractual relations with end-users, in European Journal of Law and Technology, vol.5, nbr.1,(2014).

9 Michel, Datensicherheit und Datenschutz im Cloud Computing. Fallstudie und kritische Analyse, 2.4.1ff., (2013).

Easy accessibility, most clouds are empowered by the internet and can be accessed from all around the globe.[10]

The risks of cloud-computing are: Lack of control, by committing personal data to a system managed by a cloud provider, clients may no longer be in exclusive control of their data and cannot deploy the technical and organizational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, invulnerability and portability of the data.[11]

Transparency, a lack of transparency can be caused by insufficient information about a cloud service's processing operations. This poses a risk to controllers as well as to data subjects.

Private international law, the problem which law is applicable to processing in different geographic areas and third countries.[12]

1.3 Service provision models of cloud-computing

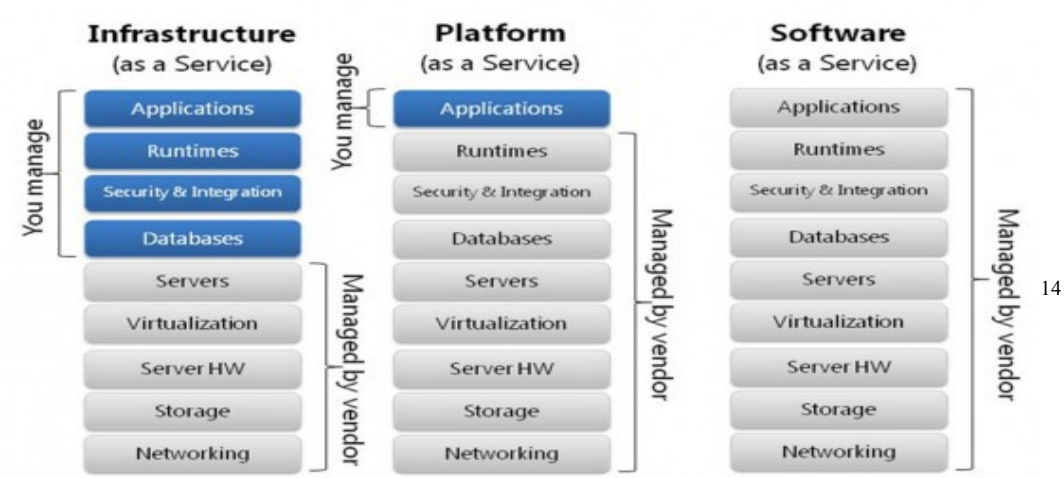
There are three different service models of cloud-computing, Infrastructure as a Service (IaaS) Platform as a service (PaaS) and Software as a Service (SaaS). In those models the user has to manage and configurate the operating systems and software to different degrees. The IaaS is the one where the user is nearly completely free and only bound to the infrastructure where in the SaaS the provider determines all the means.

In the service model SaaS is often nothing installed or saved on the users own computer. The service is directly usable by the end consumer via the internet browser.

An example for this is: the bundle of google software like: Gmail, GoogleDocs and GoogleCalendar.

SaaS is the most frequently used cloud-computing model.[13]

[10] Kian, Cloud Computing - Herausforderung für das Rechtssystem,(2016), p.16.
[11] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.5.
[12] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.12.
[13] Computerweekly.com, SaaS remains most popular form of cloud computing for UK IT,(2013).



[14]

1.4 Rollout models of clouds

There are four major rollout models of cloud-computing the private cloud, the public cloud, the hybrid cloud and the community cloud.
The private cloud enables the user to use a kind of datacenter on a cloud architecture basis. He uses the cloud completely alone.

There are two kinds of private cloud: (1) the cloud user and provider are the same person, (2) an external cloud provider which aims his services at clients.[15]

The whole cloud is under control of the one who uses it. All the resources belong to one client which accesses the cloud over a Virtual Private Network (VPN).

The exclusivity of this cloud leads to non-utilization or under-utilization. The characteristic of flexibility and unlimited scaling of resources are not given.[16]

In contrast to the private cloud the public cloud in which the resources are shared by an unlimited number of persons. The users can not decide with which other person they share the same physical infrastructure. The cloud is always provided by an external undertaking, which takes care of the control and maintenance of the infrastructure and software. Accessed is the cloud over the commonly used internet.[17]

The public cloud is the main manifestation of cloud-services. With the public cloud comes great flexibility and scalability, cost efficiency and accessibility. But also with the number of servers and users all over the world a high risk of data protection infringements.

[14] Frampton, The diffrence between IaaS, SaaS and PaaS,(2013).
[15] Bedner, Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung,(2013), p.33.
[16] Höllwarth, Cloud Migration,(2011), p.60f.
[17] Höllwarth, Cloud Migration,(2011), p.60f.

Hybrid forms of cloud computing can be compositions of private and public clouds, the user can use some resources in form of a private cloud, for higher security and other resources in form of a public cloud for high flexibility.[18]

In community clouds do users with the same interests share a cloud. They have for example the same imagination of security, quality of resources etc.. It is comparable to a public cloud for a certain group of people.[19]

2 Legal frameworks

There are two main regulatory frameworks playing a major role on the field of the relation between controller, processor and sub-processor, the DPD and the GDPR. Those two sets of rules have a major influence on cloud-computing cases.

2.1 The DPD

The DPD was introduced 1995. It stipulates one of the big steps for data protection rights after the Convention no.108.[20] It describes minimum standards of data protection which all member states have to guarantee by national law and laid down the basis for case law by the ECJ which further developed main data-subject rights like: the right to be forgotten[21].

The two main goals are: (1) to enhance the common digital market in the EU and (2) the protection of individual rights.

Whether the Directive includes a full harmonizing character is controversial.[22] But out of the reason that it is only a Directive[23], it can be concluded that it can not contain a full harmonizing character. Contrary led the DPD to a fragmentation of data protection rights in Europe.[24]

---

18 Pachghare, Cloud computing,(2015), 2.5.4.
19 Pachghare, Cloud computing,(2015) 2.5.3.
20 Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,(2013), p.9ff..
21 ECJ, C-131/12.
22 ECJ, C-101/01.
23 Directives need an implementation act into national law.
24 Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,(2013), p.9ff..

2.2 The GDPR

On the final text of the GDPR was agreed in April 2016 and it will enter into force after a two-year transition period, on the 25th of May 2018.[25]

When the Regulation enters into force it will replace the DPD. It is intended to strengthen and unify data protection for individuals in the EU, by also addressing the export of personal data.

In the first recitals is further laid down that the data protection Regulation should be simplified in the whole EU to make it easier to conduct a business and to enforce data-subject rights across the EU.

It is important to note that the GDPR is a Regulation and does not require to be transferred into national law to be applicable, as the Directive before.

The GDPR will address the fragmentation problem triggered by the DPD, and contains a greater harmonizing character.[26]

2.3 Processing

Processing is defined in Art.2(b)DPD as: *any operation or set of operations performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*

The GDPR defines in Art.4(2) Processing as: *any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

The words in the definitions are slightly changed but those amendments will probably not result in a practical difference.[27]

[25] Bird&Bird, GDPR – Timeline.
[26] Heimes, Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification.
[27] Gabel/Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU`s new data protection law,(2016), chap. 5.

Processing must under both legal frameworks be executed lawfully. To be lawful the processing needs to be conform with the main data protection principles of the EU data protection law.

Those principles are the principle of transparency, purpose specification and limitation, erasure of data and data security which contains: availability, integrity, confidentiality and accountability.

Transparency does mean for cloud-computing that the cloud client is made aware of subcontractors and the location of all the data centers his data is processed to.[28]

The principles of purpose specification, limitation and erasure of data guarantee that data is only used for the purpose it was collected and not repurposed. It is the cloud-clients responsibility to erase data as soon as necessary.[29]

The risk of personal data being processed further than the initial purpose can be assumed as being quite hight, because of the high number of processors and sub-contractors.[30] Potential risks grow with a higher number of entities involved.

The cloud-client is according to the data security principle responsible that the data is processed and available and secured from potential loss, has integrity and can not be alternated, is confidential by the usage of security measures for e.g.: encryption and be aware of being accountable.[31]

The principle of data security is named in nearly every article by referring to “appropriate measures” to comply with the Regulation.

2.3.1 Outsourcing

Outsourcing is the process of partly or complete outplacement of one business branch to a external third party.[32] It is further described as the opposite of processing.[33] There are two theories which want to determine when outsourcing is given.

[28] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.11.
[29] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.11f..
[30] Stitilis/Malinauskaite, Compliance with basic principles of data protection in cloud computing: the aspect of contractual relations with end-users, in European Journal of Law and Technology, vol.5, nbr.1,(2014).
[31] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.14ff..
[32] Oxford Dictionary of English,(2010).
[33] Datenschutz Praxis, Wichtige Datenschutz-Begriffe, Was genau versteht man unter Funktionsübertragung?, (2015).

The theory of transfer of function states: outsourcing is given when the receiving entity is not carrying out supportive services. The entity is responsible for a whole function of the superior entity and is provided with own decisional rights.[34]

The contractual theory determines: by solely looking at the assisting character stipulated in the contract of the receiving entity. If the receiving entity is under the authority of the superior entity, there is no outsourcing.[35]

Both theories differ marginally. By only differing, on which link it can be determined if the receiving entity is still under instruction of the superior entity.

If outsourcing is given both theories accord that the entity is self-responsible and liable, as controller, where as in processing cases the controller stays responsible.[36]

Examples for outsourcing are lawyers or tax advisers, they are not under the authority of the superior entity and carry out their tasks without being bound by instructions.[37]

In contrast to the regular cloud can the outsourcer always determine where his data is, while the user of a cloud does only know, which provider processes his data, but not where the physical location of the servers are. Outsourcing is not that flexible as the normal cloud. Usually there is only one third party. Continuing is outsourcing not that cost efficient, because the contracts normally demand a monthly fee instead of a pay what is used settlement (used memory space).[38]

The average cloud user does not know the difference of outsourcing and processing. The user just wants to use external computing power and does not want to manage how the computing should be done. In the majority cloud-computing cases are cases of processing.[39]

Under the Directive is no legal backing when outsourcing is given and when not. The literature tried to highlight the boarders of the definition of processing with the two theories above. In many cases is the border blurred and it can not clearly be stated if processing or outsourcing is given. It is also clear that with the help of interpretation and juristic tricks you could get the conclusion you want, leading to legal uncertainty.[40]

---

34 Gola/Schomerus/Gola/Klug/Körffer, BDSG Bundesdatenschutzgesetz Kommentar, vol.12(2015), § 11.
35 Externe Dienstleister und Datenschutz,(2015).
36 Stumper, Abgrenzung Auftragsdatenverarbeitung – Funktionsübertragung,(2014).
37 Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Auftragsdatenverarbeitung und Funktionsübertragung,(2012), p.4.
38 Abu-rab/Baun/Kunze, Kostenvergleich: Cloud Computing versus Hosting-Angebote, in iX(12/2011), p.126-130(126).
39 Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.272.
40 Steinle, Auftragsdatenverarbeitung bs. Funktionsübertragung – Teil 2: Unterscheidungskriterien,(2012).

The Regulation does not directly address the problem. The main reason to establish outsourcing was to move liability. But through making the processor liable (Art.82GDPR) and trough stating in the law that, where the processor determines the purpose of processing he shall be considered to be controller for that processing, Art.28(10)GDPR The problem of outsourcing should still exist, but the practical scope of application be smaller.

Under the GDPR the criteria of consent or instruction could be used to determine if outsourcing is given or not. Processing outside the instruction could still be considered to be outsourcing.[41]

2.4 Controllers and processor

The terms of controller and processor are basic concepts in the field of data protection law a clear definition and how the definition changed is important to understand their position in the construct of cloud-computing.

2.4.1 Controller

The term of controller is under both frameworks from high importance, the party who is considered to be controller is responsible for ensuring compliance with the law.[42]

The DPD defines controller in Art.2(d) as: *the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.*

The definition is divided in the elements “determines”, “purposes and means of processing” and “natural person, legal person or any other body” and “alone or jointly with others”.

“Determines” shall stem from the factual elements of the circumstances of the case. The questions needed to be asked, to find out if somebody “determines” are: who sets the purposes?, If processing is taking place?, Who initiated it?.[43]

---

41 Plath, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition,(2016), p.1140.

42 Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"(00264/10/EN WP 169), p.20, Art.24GDPR.

43 Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"(00264/10/EN WP 169), p.7f..

In the element of "purposes and means of processing" the dictionary defines purpose as the intended or desired result, aim, or the reason why something exists.[44] The purpose is the "why" and "how" of processing.[45]

Whereas the two remaining elements are self-explaining "natural person, legal person or any other body" and "alone or jointly with others".

Art.4(7) of the GDPR defines controller as: *the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller or the criteria for nominating the controller may be designated by those laws.*

Except from the part "or the criteria for nominating the controller " the definition is the same. Every entity considered to be a controller under the DPD is likely to be controller under the GDPR.[46]

2.4.1.1 Controller`s obligations

The fact that a party is considered to be controller is connected to a list of obligations which characterise the controller-status.
The principle of accountability is ought to ensure the enforcement of the main data protection principles.

Under the Directive, Art.6(2) only the controller is accountable. He must ensure compliance with the main data protection principles, when processing.

Whereas under the GDPR the controller is not only accountable, but must also be able to demonstrate compliance with the main data protection principles, Art.5(2),rec.85.

The measures to demonstrate compliance have to be "appropriate technical and organizational measures" and codes of conduct, Art.24GDPR.

The GDPR tries to set down criteria in rec.74GDPR to determine what a appropriate measure could be. The controller should take into account the nature, scope, context and risk to the rights and freedoms of natural persons.

---

44 Oxford Dictionary of English,(2010).
45 Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor"(00264/10/EN WP 169), p.7f..
46 Gabel/Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU`s new data protection law,(2016), chap. 5.

A manifestation of the accountability is the obligation, in Art.30GDPR to keep records of all processing activities to proof compliance with the obligations and main data protection principles.

The other obligations are the following: liability, appointment of processors or reporting data breaches.

It is a minus for enterprises that they need to show compliance under the GDPR compared to the DPD, it means an extra of effort and costs. On the other hand does the GDPR provide information how demonstrating compliance could be done and how "appropriate measures" need to be chosen.

The tenet of data protection by default and by design means: that data protection is not something you take care of after you developed a new software or product. Data protection should be a key element in the process of planning and building new software and products.[47]

The GDPR obliges controllers to implement measures of safeguard in every planning or processing phase of every new product or service, Art.25,rec.78.

Whereas the DPD does only oblige the controller to protect the main data protection principles not specifically obliging to involve them into every phase of planning and building a product.

Data protection by design and default can be a big burden on developers. But enhances the protection of individuals.

Entities acting as controller usually appoint other service providers acting on their behalf (processor), to process data. This is not prohibited under the law but most follow certain rules. Among others the controller does need to choose providers under consideration of certain criteria laid down in the law.

The Directive lays down those criteria in Art.17(2)(3). A controller is only allowed to appoint a processor, which can guarantee compliance with the law and the main data protection principles. The appointment has to be a contract in writing and shall stipulate that the processor is acting on instruction of the controller.

The GDPR only allows controllers to appoint processors which ensure compliance with the law but further does the contract need several laid down requirements, which will be shown later, Art.28(1)-(3),rec.81.

[47] Gutwirth/Leenes/De Hert, Data Protection on the Move: Current Developments in ICT and Privacy/Data, (2016), p.137.

When appointing processors, the GDPR imposes significant new requirements, especially to the contract, which could make it harder for controller to choose appropriate processors. It could happen that processors outside the EU resist the new obligations and make negotiations even harder for the controllers.[48]

To prove compliance with the data protection law, to the data protection authorities, it is possible to keep records of processing activities.

The Directive obliges the controllers to notify the supervising authority before the processing of personal data, Art.18,rec.48DPD. This notification requirement can vary from member state to member state.

Instead of notifying the supervising authority the GDPR requires controller to keep record of the controllers processing activities, Art.30rec.82ff.GDPR, including: the contract details, the categories of data, the purpose of the processing, information regarding cross border data flow, information about the security safeguards and data retentions periods.

The exemption in Art.40(5)GDPR states that organizations employing fewer than 250 persons are exempted from the obligation to keep records, except the processing results in a high risk for data subjects.

Those records must be shared with the data protection authorities if requested.

The obligation to record processing activities is new under the GDPR, which makes it easier for controllers to start processing but still keeps the possibility for the supervising authorities open to control the controllers and intervene. The burden to notify the supervising authority every time personal data is processed does not exist under the GDPR. The obligation shifts from a pre-processing control to a post-processing control making it easier for undertakings to start in the market.

This also reduces the administrative burden on the controllers. With the one-stop Shop concept, the key feature of the new Regulation,[49] controllers, which act in several countries, can choose one single leading supervising authority and get all the necessary permissions from that.

The exclusion for undertakings under 250 employees is only comprehensible in the way that it would be a high financial burden on smaller undertakings but not even the recitals make clear why it is at 250 and not a different number.

[48] Gabel/Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU`s new data protection law,(2016), chap. 10.

[49] Bracy, Article 29 Working Party lays out GDPR action planhttps,(2016).

The Directive requires in Art.17DPD, that controllers must implement appropriate technical and organizational security measures (safeguards) to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

The GDPR includes the wording of the DPD but further states that depending of the nature of processing the safeguards may include: pseudonymisation and encryption, the ability to ensure ongoing confidentiality, backup mechanisms, and regular testing of the safeguards.

On the point of data security does the Directive use a open formulation which leaves room what is appropriate or what is state of the art. The Regulation is more prescriptive. The prescription character of the GDPR can be a problem in the way that it can someday be considered to be not technological independent.

To take actions against breaches of the law the data protection authorities need to know when and who committed them. Therefore it is important that controllers report those breaches.

The Directive did not know such an obligation and left it to the member states to implement such a notification requirement.

New under the GDPR, Art.33, is that controllers must report breaches to the DPA without undue delay within 72 hours, but not when the breach is unlikely to result in any harm to data subjects. The Notification must contain a prescribed minimum content. Laid down in Art.33(3)(a)-(d)GDPR: (a) description of the data breach, nature and number of data subjects involved, (b) the name and and contact detail of the data protection officer or point where information can be obtained, (c) the consequences of the breach and (d) the measures taken by the controller to address the data breach.

Additional the controller needs to document breaches and enable those documents to the supervising authorities.

The burden will be bigger for the controllers under the GDPR out of the reason that there was no such obligation under the DPD. Especially the 72h deadline can be extremely challenging as well as the obligation to keep records for every data breach no matter how small it was.

Data subjects must be notified by the controller in the case of a data breaches, when it is from an high risk for it, Art.33GDPR. The regular data subject does not have the knowledge or technical measures to recognize data breaches. By establishing the obligation of notifying data breaches to the data subject this disadvantage can be outweighed.

The Directive does not oblige controllers to notify data subjects and leaves it open for the member states to establish such an obligation.

Art.34, GDPR introduces this obligation. When data breaches impose a high risk to data subjects, controller need to notify those data subjects without undue delay.

The communication to the data subject must contain the same content as the communication to the supervision authority.

This duty does further enlarge the burden on the controller by obliging him to take more organizational measures to full fill it. Through communicating data breaches to data subjects the possibility of reputation harm arises. But this harm should not occur if the controller follows the law. Further the time limitation is even tighter than for notifying the supervising authority and not nearer explained what "high risk" and "without undue delay" actually is.

It is a new obligation under the GDPR that controllers must appoint data protection officers, which monitor, if the controller complies with the GDPR, Art.37ff.GDPR.

The term of controller is more relevant under the GDPR than under the DPD because it is connected to stricter and new obligations.[50]

Under the GDPR the rights of the data subject are enhanced and the main data protection principles better guaranteed than under the DPD.

The fragmentation of requirements in the different member states under the DPD is solved.[51]

2.4.1.2 Joint controllers

If more than one entity determines the purpose of processing they should be considered to be joint controllers

The DPD does not use the exact term of joint controllers but acknowledges the concept. It is contained in the definition of controller in Art.2(d)DPD, which states:"natural or legal person, which alone or jointly determines the purpose".

The liability of joint controllers in the DPD is regulated in Art.23,rec.55. Which also allows a exemption from liability if one controller can prove that it is not responsible for the event, which caused the damage or for the case of force majeure.

On the other hand the Regulation directly addresses joint controllers in an own definition in Art.4(7),rec.7:"*Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers*".

[50] Gottlieb, The General Data Protection Regulation: Key Changes and Implications,(2016).
[51] Gilbert, EU General Data Protection Regulation: What Impact for Businesses Established Outside the EU, (2016).

Joint controllers need to have an arrangement between them, which allocates the responsibilities, Art.26GDPR.

The essence of the arrangement shall be made available to the data subject and the data subject may exercise his or her rights against each of the controllers, Art.2(2),(3).

Under the GDPR each joint controller is liable for the whole damage and a controller can only be exempted form being liable, if he can prove that he is not in any way responsible for the damage. If one controller is exempted the other joint controller has to recover the whole damage, Art.26,82,rec.79,136GDPR.

In complex structures of processing, such as cloud computing, some entities may not realize that they have become joint controllers, by determining the purpose of the processing activities jointly, and have to be on the watch to comply with all obligations addressed at controllers and to enter into arrangements with each other and make this arrangement public to the data subject.

This state of being on the watch may be intended by the GDPR to make sure entities are monitoring their processing all the time , to avoid serious compensation claims.

The DPD exempts controllers from liability in cases of force majeure, the stricter GDPR does not. This results in a liability of the controller for every kind of scenario like natural disasters. This goes beyond every reasonable liability, force majeure cases are usually exempted in terms and conditions.

Anyway it is a disadvantage for joint controllers that they are liable in form of a full compensation to the data subject under the GDPR.

2.4.1.3 Determining who is controller in cloud-computing

In the majority of transactions between service providers and customers, the legal obligations and responsibilities for each party are clear.

In cloud computing cases this can be more complicated, especially concerning the data privacy obligations.

The cloud-service provider has huge influence on important decisions about the conditions of processing, such as where the information is stored, the use of sub-processors and security.[52]

[52] European Data Protection Supervisor, Q&A 10) Cloud Computing.

Considering that a private person usually does not know a lot about computer science or the complexity of clouds, it appears to be a possibility that the service provider may be the controller

But the Art.29 Working Party follows strictly the definitions, stated in the DPD, for controller and processor.

Following the definition of controller in Art.2(d)DPD the cloud user decides on the "if", a third party is used and on the "how" of processing. In other words the user determines the purpose of processing.

It is the user who determines,[53] which data should be uploaded to the cloud and what he wants to achieve with that.

The cloud client therefore acts as a data controller. The cloud user as controller is recipient for the duties shown above.

This is in accordance with the efficiency and flexibility character of clouds.

The cloud-provider is the body, which provides a platform based on one of the models shown above, in cloud computing mostly SaaS. When the provider acts on behalf of the cloud-user the provider is following the definition in Art.2(e)DPD considered to be a processor.[54]

The Art.29-WP further states that as a matter of fact, there may be individual cases in which a cloud-service provider can be considered either as a joint controller or as a controller depending on specific circumstances. This could be the case where the cloud provider processes data for its own purposes.[55]

The Status "controller" or "processor" is not statical determined on a certain date for the rest of the processing. It must be reconsidered with every single processing act.[56]

It is important to note that in complex processing tasks, where different parties take part in processing compliance with the law and especially the responsibilities for data-breaches must be clearly allocated to prevent a undermining of the main data protection principles.

In the majority of cloud-computing cases, clients can not negotiate the contractual terms of the cloud-service. The contracts are mainly standardized and leave the client in a take-it or

---

53 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.7f..

54 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.7f..

55 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.7f..

56 Jotzo, Der Schutz personenbezogener Daten in der Cloud,(2013), p.70ff..

leave-it position.[57] Even though the client has less contractual power against the big provider does this not justify the controller to accept contracts which are breaching the DPD. The controller is obliged to choose a cloud provider that guarantees compliance with data protection legislation.

Nevertheless the client determines the purpose of that processing and is considered to be controller and therefore has to ensure the compliance with the law.[58]

Since the definition of controller stays substantially unchanged, the assumption is that also under the GDPR cloud-clients are controllers.

2.4.2 Processor

The DPD in Art.2(e) and the GDPR in Art.4(8) use the exactly same definition of processors: *a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.*

On the point of application of law does the Directive not address processors as such. The Directive only requires, in Art.4(1)DPD, all member states to implement direct legal obligations on controllers, which fall in the scope of the Directive.

Whereas the GDPR applies to a controller or processor, regardless of whether the processing takes place in the EU or not, Art.3(1).

The scope of the GDPR is exponentially wider than the one of the DPD.[59]

2.4.2.1 Processor`s obligations

New under the GDPR is that, when the likely case appears that the instruction by the controller is in conflict with the EU law. The processors is required to immediately inform the controller in case they believe that the controllers instruction is violating EU law, Art.28(3),33(2)GDPR.

The dilemma for the processor of either fulfilling the contract with the controller or following the law is now solved. The controller has to find ways to give his orders lawfully.

---

[57] Hon/Millad/Walden, Negotiating cloud contracts: Looking at aclouds from both sides now, in Stanford Technology Law Review, Vol.16(1/2012), p.89.

[58] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.20ff..

[59] De Hert/Czerniawski, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context,(2016), p.1.

The Directive allows processors to appoint sub-processors as long as the processors act within the scope of the instruction given by the controller. If they can appoint sub-processors these also have to act within the scope of the instruction given by the controller, Art.16,17DPD.

The Regulation also allows processors to appoint sub-processors, but only with consent of the controller and depending on the form of consent, the possibility for the controller to intercept. The sub-processor must meet the same requirements as the processor, Art.28,(2),(4).GDPR

The foreseeable case that a processor may not comply with the instruction of the controller is not specifically regulated under the Directive. According to the Directive their contract decides what happens.

If a processor infringes the Regulation by determining the purposes and means of processing the processor shall be considered to be a controller in respect of that processing, Art.28(10)GDPR and therefore liable. This is also ensured by Art.82(2)GDPR.

One of the biggest changes is the liability for data protection law breaches. Under the DPD is the processor liable only in the relation to the controller based on the contract they concluded. Data subjects can not claim the processors.

In opposite under the the GDPR. Processors can directly be claimed by data subjects

The processor is liable when he breaches the GDPR or acted outside the instruction given by the controller.

The penalties can be up to 20m euro or 4% of the annual worldwide turnover, Art.82,83GDPR.

Further new under the GDPR is that each processor (and its representative, if any) must keep records of its processing activities performed on behalf of the controller Art.30(2). Also it is new that processors must report data breaches and when meting the requirements appoint a data protection officer, Art.33,37GDPR. Processors have to meet the same safeguards for processing as controllers, Art.28GDPR.

Those new obligations for processors are interpreted to be anti-commercial, because it means a higher need of management for the processors and with that higher costs.

The border between controller and processor under the GDPR is not that clear as it was under the DPD. Now nearly the same obligations apply to both.

It is a big change keeping in mind that under the Directive where processors were just helping entities for the controller which where only liable in the contract with the controller and where only target to small obligations.

The Regulation recognizes that the DPD was a toothless tiger on the point of processors and that a lot of data subject rights infringements arose because of the large number of processors, especially in cloud-computing cases. That personal data is the oil of the 21th century seems to have an influence on the law-making.[60]

The GDPR full fills it goals to strengthen and strictly enforce data subjects rights and the main data protection principles.

2.4.3 Sub-processor

The services do not necessarily need to be executed by the processor, the processor can use the services of third parties, namely, sub-processors.[61]

Sub-processors are defined in the Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under the DPD.[62]

The Decision does only apply to processing to third countries, but with the aim to establish with standard contractual clauses an adequate level of data protection there as the DPD did in Europe.

Even if the Decision does not directly apply, and mainly repeats the text of the DPD, it does allow a peek how the Commission wishes how the obligations under DPD should be fulfilled in the relation to sub-processors. It can be seen as an amendment to the DPD.

The Art.29 Working Party also referred on the point of sub-processing to the Decision and recommends the usage of nearly the same contractual terms for processing in the EU.[63]

By definition a sub-processor is: *any processor engaged by the data importer or by any other sub-processor of the data importer and who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for the*

---

60 Haupt, "Data is the New Oil"—A Ludicrous Proposition Natural resources, the question of ownership and the reality of Big Data,(2016).

61 Schulz, Cloud Computing in der öffentlichen-Verwatlung, Chancen - Risiken – Modelle, in MMR p.75(79).

62 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU.

63 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9f..

processing activities to be carried out on behalf of the data exporter after the transfer in accordance with the data exporter's instructions, Art.3(e).

The Data importer means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf, Art.3(d).

Art.3(c) defines data exporter as the controller who transfers the personal data.

It allows to replace the words data importer with processor and the word data exporter with controller and read the definition for the EU data processing like: *sub-processor is any processor engaged by the processor or by any other sub-processor of the processor and who agrees to receive from the processor or from any other sub-processor of the processor personal data exclusively intended for the processing activities to be carried out on behalf of the controller after the transfer in accordance with the controllers instructions*.

The GDPR does not define sub-processor but acknowledges the construct in Art.28(2),(4) and establishes some obligations. Further does the Regulation not differ in the wording between processor and sub-processor. The wording "where a processor engages another processor", is used to describe the concept of sub-processors. This is contentual the same as the definition given by the Commission Decision[64].

3 Relation between controller and processor

There are three kinds of relations in cloud-computing cases. The relation between the client/controller and the processor, the relation between processor and sub-processor and the heavily discussed relation between controller and the sub-processor. To get to the core of the thesis: the relation between controller and sub-processor, Will first the relations of controller to processor and processor to sub-processor be shown.

3.1 Relation between controller and processor under DPD

The relation between controller and processor is shaped by the contract, which sets minimum criteria and by the duties/rights of control, selection and decisional authority. Both those criteria are mandatory and set down in the law.

[64] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU.

3.1.1 Contract

3.1.1.1 Form of the contract

The Contract requires the form of writing or equivalent form, Art.17(4)DPD. The criterion of written form fulfills several functions: function of proof, warning function and function of control.[65]

The function of proof and control provides the parties with the possibility and security to proof compliance, with the contract and control what was negotiated in the contract.

Out of the warning function element of the form requirement follows that the contractual parties have to conclude the contract with special care and attention. When a contract needs to be in writing a natural person is more concerned about the content of the contract. The written form implies that with the conclusion of the contract their rights can be affected in a big scale.

3.1.1.2 Content of the contract

The contract shall stipulate in particular that the processor shall act only on instruction from the controller. It needs to contain the criteria laid down in Art.17(1), Art.17(4)DPD, and shall mainly stipulate that the processor need to follow the main data protection principles.

The contract has to contain according to Art.17(3)DPD contain: a term which states that the processor shall act only on instruction from the controller and that the processor must fulfill the obligations in Art.17(1)DPD: implemented appropriate technical and organizational measures to protect personal data.

Additional it is not allowed to exclude the data subjects rights in Art.13ff.DPD but it can be allowed to restrict those rights depending on national law. The data subject`s right to object, Art.14DPD, is not in the list of Art.13DPD and must be guaranteed.

The national legal frameworks can vary on the following point, but it seems that the majority of countries agreed that the term of "organizational measures" in Art.17(1)DPD must be interpreted in the way that: the contract shall contain all means of how the right to control of the controller can be executed and to which extent.[66]

---

[65] Geis, Ein Rahmenwerk für den elektronischen Rechtsverkehr: Zugleich ein Beitrag zur Modernisierung gerichtlicher Verfahren dargestellt am Beispiel der Verwaltungsgerichtsbarkeit Rheinland-Pfalz,(2014), p.101.

[66] Brennscheidt, Cloud Computing und Datenschutz,(2013) p.122ff.

Especially for cloud-computing cases is the allocation and extend of rights important. Through a lack of transparency it can be hard for the controller to fulfill this duties (ensure compliance with the law), so that a contractual term, how to conduct his duty of control, is from importance.[67]

The contract can also stipulate how far the decisional authority over the processor reaches and how far the self determination right of the processor is protected.

In cloud-computing is the majority of cases between a big undertaking and a lot of private persons. To follow each individual instruction is impractical for the processor. Especially for those cases it is important to determine the scope of the decisional authority.

In addition did the Art.29 Working Party recommend contractual safeguards for the relation of controllers and processors.[68] The recommendation of the Working Party is not legally binding but the contract shall among other terms contain terms governing the follow issues: (a) details on the extent and modality of the clients instruction, (b) specification of security measures, (c) the purpose of processing as well as the types of personal data being processed, (d) specify how the personal data will be retained afterwords, (e) a confidentiality clause, (f) how the data subjects right of access is guaranteed , (g) sub-processors may only be engaged with consent with the possibility to object and the contract between the SP and the P must guarantee the same data protection level as the contract between C and P, (h) notification of data breaches.[69]

3.1.1.3 Standard contracts

Big entities on both side of the contract can negotiate individual contracts. But the majority of cases in cloud-computing is between private persons and an undertaking providing the cloud.

Using standardized contracts and terms and conditions is in the interest of cloud providers and cloud users. The cloud providers do not have to take care of every individual instruction. Standardized contracts assure the efficiency character of the clouds.[70]

---

67 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9f..

68 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.12ff..

69 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), sec.2.4.2.

70 Brennscheidt, Cloud Computing und Datenschutz,(2013) p.125f.

3.1.2 Selection and control of processors

The obligations to select and control derivates out of Art.17DPD. It is on the controller`s behalf to control and choose a processor. The processor must provide sufficient guarantees in respect of the technical security measures and organizational measures governing the processing and must ensure compliance, Art.17(3),rec.46DPD.

The controller must not choose the one, which provides the highest standard of data protection, only the standard set down in the law must be met.[71]

How far the obligation of selection and control reaches is controversial as well as in which time intervals they have to be fulfilled.

The EU did not legislate how detailed the controls needs to be or in which interval. The EU uses the open formulation of "state of the art" and "appropriate", which leads to national fragmentation. The Working Party wants this to be settled in the contract.[72]

The obligation of control and selection exist in parallel.[73] Argument for that is the wording in Art.17(2)DPD, which introduces them in one sentence. Only when the controller informs himself (control-right) can he fulfill the obligation to select a satisfying processor. There are no different requirements for each of the rights.

That implies that the controller has to ensure that the processor complies with the main data protection principles, when he selects a processor or when he controls a processor.

The principle of data security demands that the data is protected from external threats. The core of both duties is to ensure that there is adequate protection from those threats. In an individual case could that mean that the controller must visit the physical location of the cloud servers, ask for the standards of encryption and how the data is protected against hacking-attacks.[74]

This requires a high knowledge of computer science and can not be expected from every controller.

---

71 Plath, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition,(2016), p.423.

72 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9.

73 Bergmann/Möhrle/Herb, Datenschutzrecht Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz,(2016), §11BDSG.

74 Brennscheidt, Cloud Computing und Datenschutz,(2013) p.123..

3.1.3 Decisional authority

Decisional authority is in abstract the right, power to give orders, instruction or to practice rights against someone.[75]

The decisional authority is stated in Art.17(3)DPD "The processor shall only act on instruction of the controller".

A strict interpretation of the word instruction defines a instruction as: the order from the principle to the agent to execute a certain action.[76]

Such a approach is in cloud-computing relationships from private persons to entities inconceivable. Especially if the contract was formed through a standardized agreement.

A wider approach sees an instruction as the opening of a frame in which the processor can act.

In this approach the processor still has room to operate independently.

It is important that the processor stays within the scope of the instruction and contract given by the controller. But also that those instructions leave room for independent decision making to assure the efficiency advantage of cloud-computing.

3.1.4 Liability

The Controller is responsible for all actions of the processor and liable for them.[77]

If the case appears that the processor acts against one of the controllers instructions, the common sense would decide that the processor should be responsible for its actions. But the Art.29 Working Party states that for such cases the controller and the processor are joint controllers.[78] Argument for this is the in the DPD implied distribution of risks, that only controller can be held liable.

3.1.4.1 Determining how the duties of control and selection can be fulfilled

The intensity of the control is depended on the kind of data processed.

There are different interpretations and understandings how detailed and to which extend especially the right of control must be executed. All forms of interpretation are compliant with

[75] Oxford Dictionary of English,(2010).
[76] Brennscheidt, Cloud Computing und Datenschutz,(2013) p.130.
[77] Art.17(1)DPD, Art.23DPD.
[78] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.7f..

the law some are more practical than others and some are more compatible with the nature of the cloud-computing than others.

3.1.4.1.1 Strict interpretation

A strict interpretation of the wording "the controller must ensure" would lead to a scenario in, which the controller would have to visit and inspect every data centre in person, to be sure that the measures for complying with the law and to protect the data are made sufficiently.[79]

For cloud computing is this compared to outsourcing absurd. In outsourcing cases just one data-centre is affected. In cloud-computing could it happen that there are over 100 data-centers affected situated all over the globe. Further the usual cloud controller does not have the knowledge to do a appropriate inspection of IT infrastructure or software.

The consequence is that it must be allowed that a third person can do the control and selection.

3.1.4.1.2 Third party assessment

So some people in the literature hold the opinion that the cloud user can delegate a third person, a expert, to fulfill the duties of control and selection.[80] This is a known figure in the DPD comparing with Art.20,rec.54DPD. This brings the advantage of less effort and less need of IT-knowledge for the undertaking but for a single user is the usage of an expert extremely expensive.[81]

The impractical disadvantage can be outweighed if the result of the experts inspection is shared with several cloud users.

3.1.4.1.3 Certificates

The next opinion how the controller can full fill its duties of control and selection is to share the results of expert inspections in forms of certificates.

A certification mechanism is a way of demonstrating that you comply, and implemented technical and organizational measures and safeguards.[82]

---

79 Petri, in Smitis Bundesdatenschutzgesetz, 8.edition,(2014), p.929.

80 Heidrich/Wegener, Sichere Datenwolken – Cloud Computing und Datenschutz, in MMR(2010), p.803(806).

81 Borges/Brennscheid, in Borges/Schwenks Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce,(2012), p.43(67).

82 Gabel, in Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, (2013), p.458.

Extern third parties would examine the infrastructure, software and safeguards of an cloud-service provider and would testify the compliance with an certificate. The controller would fulfill his duty by just checking the certificates by authorized certification bodies.[83]

There is no legal obligation under the DPD to get certificates but in practice are already seals available like the European Privacy Seals (EuroPriSe), which is given to IT-services and IT-products, and other certifications on national level.

It can also be thought of certificates that are awarded on the standardized contracts and terms and conditions between controller and processor.

Even though the EU-Law does not require a certain interval should the certifying body recheck if the requirements are fulfilled over time. The EuroPriSe for e.g. must be renewed every two years.[84]

3.1.4.1.4 Codes of conduct

The DPD establishes codes of conduct in Art.27DPD. These codes, where in practice just from small importance, which comes from the vague wording in the relevant article. There are no clear recommendations how codes of conduct should be approved or what the criteria to approve them are.[85]

3.2 Relation between controller and processor under the GDPR

The relation between controller and processor under the GDPR must be governed by contract or other legally binding act under EU member state law, Art.28(3)GDPR.

3.2.1 Contract

3.2.1.1 Form of the contract

The formal requirements for the contract between controller and processor are: that the contracts needs to be in written form. This includes electronic forms under the GDPR, Art.28(9)GDPR.

---

[83] Petri, in Smitis Bundesdatenschutzgesetz, 8.edition, p.930.
[84] Meissner, Zertifizierungskriterien für das Datenschutz Gütesiegel EuroPriSe, in DuD(2008), p.525(526).
[85] Von Braunmühle, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition,(2016), p.1186.

3.2.1.2 Content of the contract

The contract between the controller and the processor must set out a minimum content which is stipulated in Art.28(3)(a)-(h)GDPR. In particular should the contract contain: (a) that the processor processes the personal data only on documented instruction from the controller (Art.29GDPR), (b) persons involved in processing have committed themselves to confidentiality, (c) the procedures assures the security of processing, Art.32GDPR, (d) the engagement of sub-processors must comply with Art.28(2)(4)GDPR, (e) assist the controller with appropriate technical and organizational measures, taking into account the nature of personal data, (f) assist the controller compliance with Art.32-36 (Security of Processing, Communication of data breaches to the data subject, Notification to the supervising authority, Data protection impact assessment and Prior consultation) (g) after the end of processing the processors must be obliged to return or delete all the data and (h) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Art.28GDPR. This list was complied under consideration of the german Data Protection Act.[86]

If contracts concluded under the DPD will still be valid under the GDPR can not be stated in general. Every contract must be accessed and may be amended. Especially the points (d) engagement of sub-processors and (f) appear to be problematic.

3.2.1.3 Standard contracts

Contracts may be based on standard clauses under the GDRP, which can be laid down by the European Commission or supervisory authorities, Art.28(6)-(8),rec81GDRP. The standardized contracts are under the GDPR a tool to guarantee data security and transparency and as under the DPD in the interest of both parties.

3.2.2 Selection and control of processors

The controller shall select only a processor providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that processing will meet the requirements of the GDPR and who ensure the protection of the rights of the data subject, Art.28(1)GDPR.

[86] Bundesdatenschutzgestezt(BDSG),§11.

Selecting a processor which can proof sufficient safeguards can only be done when the controller informs himself about the safeguards. The selection must be done under consideration of the expert knowledge, reliability and resources.[87]

The duty to control is not limited to the point in time, where the controller selects the processor. Art.28(1)GDPR can be read that this duty should be fulfilled during the whole processing activity.[88]

In addition does Art.(5)GDPR refer to codes of conduct or certification mechanisms, which are still not mandatory, but can be a helpful tool.

The whole process is similar to the DPD process.

3.2.3 Decisional authority

Like under the DPD the processor is only allowed to act on instruction of the controller, Art.28(1),Art.29rec.79GDPR. This also opens a room of maneuver for the processor.

But by introducing more obligations on the processor under the GDPR and by setting out minimum requirements in the contract, this room of maneuver is smaller and more regulated.

This does not mean for cloud-computing cases that the regularly big service providing entities must now follow all the orders of user.[89] But with in parallel strengthening the rights of the controller, and strengthening the subjective rights of the data-subject, for e.g.: Right to access, right to be forgotten etc., the “small” end-user is not so left alone in a take-it or leave it position, as under the DPD.

3.2.4 Liability

Under the GDPR are the controller and the processor liable and responsible for infringements, Art.82GDPR. Both can be claimed by the data subject.

If determining the purpose of processing the processor according to Art.28(10)GDPR shall be liable like a controller in regard to that processing action.

This exposes the processor to the major risk of paying compensations, which enhances the position of the data subject and the enforceability of the main data protection principles by

[87] Rec.81GDPR.
[88] Martini, in Paarl/Pauly Datenschutz-Grundverordnung Kompaktkommentar,(2016), p.343.
[89] The decisional authority can be cut down in the contract between controller and processor. So does the law only state in Art.29GDPR “on instruction”, a instruction can be given broadly or in general.

addressing the entity which actually breached them. One of the main principle of tort law, the interest of only being liable for the party you actually contracted with or which actually broke the law is now sufficiently implemented.

3.2.4.1 Determining how the duties of control and selection can be fulfilled

3.2.4.1.1 Certificates

Art.42GDPR establishes data protection certification mechanisms, data protection seals and marks. The purpose of those is, to demonstrating compliance with the GDPR. The certificates will be voluntary and not only controllers but also processors can get them to demonstrate the existence of appropriate safeguards, Art.42(2f.)GDPR.

Even though the certificates are used to demonstrate compliance this does not reduce the responsibilities of the controllers, Art.42(2)GDPR.

The certificates are granted by supervising authorities or certification bodies, Art.43 on the criteria by the supervising authority or the European data protection board. If the Board approves the criteria this may result in a common certification called the European Data Protection Seal.

According to Art.42(7)GDPR the certificates are granted no longer than three years, but can be renewed afterwards.

To get a certificate the controller or processor has to provide all the necessary information to the certifying entity about its processing activities, Art.42(6)GDPR.

Certification bodies are entities which have an appropriate level of expertise in relation to data protection and have accreditation by a supervising authority or the national accreditation body[90],Art.43GDPR.

The certification bodies have the power to issue and renew certificates, but is also responsible for a proper assessment leading to a certification or withdrawal of such, Art.43(4)GDPR.

To get the accreditation the bodies need to full fill the criteria of Art.43(2)(a)-(e)GDPR:

(a) demonstrate their independence and expertise, (b) undertaken to respect the criteria in Art.42(5) and approved by the supervising authority, (c) establish procedure for reissuing, periodically review and withdraw of certification, (d) establish procedure to handle

[90] Regulation (EC) No 765/2008 of the European Parlimant and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

complaints about infringements or how the certification has been implemented and (e) demonstrate that their tasks do not result in a conflict of interests.

The certification bodies does itself need a accreditation. The accreditation shall be issued for a maximum of five years and can be renewed under the same conditions it was provided, Art.43(3f.)GDPR.

3.2.4.1.2 Codes of conduct

In Art.40GDPR codes of conduct are going to be refined. Codes of conduct are known in the english and American law system and can be understood as an agreement on rules of behavior for a group or organizations[91] They manifest a form of co-Regulation.

The GDPR wants associations and other bodies which represent controllers and processors to encourage the usage of such codes, rec.98GDPR.

To be approved the codes should contain the content the points of Art.40(2)(a)-(k)GDPR: (a) fair and transparent processing, (b) legitimate interests pursued by controllers in specific contexts, (c)the collection of personal data, (d) the pseudonymisation of personal data, (e) the information provided to individuals, (f) the exercise of rights of the data subject, (g) the information provided to and the protection of children and how parental consent can be obtained,(h) the measures and procedures to assure data protection by design Art.24, the responsibility of the controller,25 and the security of processing Art.32 with their technical organizational and security measures, (i) breach notification (j) data transfers to third countries or (k) out-of-court proceedings such as alternative or online dispute resolution procedures

Codes of conduct must be approved by the supervising authority and published, Art.40(5f.)GDPR. If the code of conduct relates to processing in several member states the normally approving supervising authority shall forward the draft of the code to the European data protection board, which than can provide a opinion if the supervising authority shall approve the code, Art.40(7)GDPR.

When the European data protection board thinks the code of conduct is in compliance with the GDPR it hands it to the European commission which can make the code of conduct by implementing acts valid in general, Art.40(9)GDPR.

[91] Oxford Dictionary of English,(2010).

The codes of conduct are monitored by the supervising authority or a competent body, Art.41(1)GDPR.

The body must fulfill the requirements of Art.41(2)GDPR and has to (a) demonstrate its independence and expertise to the satisfaction of the competent supervisory authority, (b) established procedures which allow it to asses the eligibility of controller and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation, (c) establish procedures to handle complaints about infringes of the code or how the code is being implemented and (d) demonstrate to the supervising authority that its task do not result in a conflict of interest.

The codes are not enforceable but monitored Art.40(4)GDPR. The body shall take appropriate action in cases of infringement of the code of conduct, including suspension or exclusion of the controller or processor and inform the supervising authority,Art.41(4)GDPR.

The supervising authority has to monitor he conducting body, Art.41(5)GDPR.

Codes of conduct and certificates can apply in the same cases, they do not exclude each other. Certificates proof the compliance from a technical point of view, whereas the codes can determine certain manners for a product or a branch.[92]

3.2.5 New duties of processors under the GDPR

The relation between controller and processor under the GDPR is affected by two new duties, which now are established by law.

The duty to notify personal data breaches to the controller and the duty to inform the controller if an instruction is infringing, in the eyes of the processor, European law.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

The duty for the processor to notify the controller, if he will breach the law as well as the duty of the controller to notify the supervising authority and the data-subject are new under the GDPR.

The EU lend this duty from the german BDSG. This duty was implemented with the thought in mind that in the majority of cases the processor does know more about processing data, legally and technologically.

[92] Von Braunmühle, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition,(2016), p.1188.

In addition it is often not possible for the controller to notice data breaches at all.

The duties for the processor to notify the controller and for the controller to notify the supervising authority are written down in Art.33GDPR with its minimum content described in Art.33(3)GDPR.

The notice has to be made without undue delay after becoming aware or in 72 hours after. The information does not need to be provided at a time and can be provided in phases, but should be provided as fast as possible.

Minimum content is: (a) describe the nature of the data breach, with categories and number of data subjects concerned, (b) communicate the name and contact detail of the data protection officer or point where information can be obtained, (c) describe the consequences of the breach and (d) describe the measures taken to address the breach.

The duty to inform the controller about infringing instructions is set down in Art.28(3)GDPR.

The processor must immediately inform the controller if an instruction is in the processors eyes infringing the Regulation. Under the DPD this was not regulated by law but by the contract between the parties. The processor was in a dilemma either to fulfill the contract or to processes in accordance with the law.

Now is clearly regulated what to do if such a case appears. But the processing entities have to keep in mind, if the order of the controller was lawful and they do not follow it, they can be held liable according to Art.82(2)GDPR.

3.3 Comparison of the relation controller and processor under the DPD and the GDPR

The requirements to the contract under the DPD are vague. It is possible to fit cloud-computing under the current DPD, if it is used with a wide interpretation.

By not providing references in the context of cloud-computing or contractual minimum contend arose unregulated gaps.

The GDPR does like the DPD require the contract to be in the written form but also specifies to allow the electronic form, this change was made owed to the technical progress. The usage of clouds is getting easier by loosening the formal requirements (usage of electronic form). By giving right to the authorities and the commission to lay down standard clauses, users of clouds can be sure to be treated equally from provider to provider. This appears to be

convenient, because in the majority of cases the cloud-service provider is one big entity contracting with a lot of individuals. The control through the commission ensures that the usually big standardized contracts guarantee the minimum standard of data protection. The usage of rights gets easier for a single user when the contracts with standardized terms are predetermined by the commission. This provides an easier and safer way of access to clouds. The required minimum content for contract in the law shifts from just two minimum criteria to eight. The GDPR contains both DPD criterion and is more descriptive to ensure a adequate and higher level of data protection.

But when comparing the recommended contractual safeguards of the Art.29 Working Party[93], it becomes clear that most of the points from the Working Party became mandatory by law in the GDPR.

On the point of how the controllers can fulfill their duties under the DPD the possibilities are manifold. In my eyes the certification of cloud-service providers is the one with the most advantages. It is cost efficient, less effort for the individual and does not require the individual to have high computer-science skills. Is is the only mechanism, which can be thought of, that allows an application in the majority of cases.

Maybe through the age of the Directive non of such mechanisms were part of the law. Certification had with that a uncertain legal basis and is not mandatory. Especially for Cloud-computing is it a disadvantage for the end-consumer.

Under the GDPR the problem of certification is tackled.

The GDPR does leave gaps for interpretation by using vague wordings like “appropriate level of expertise”. It is clear that the legislator does not want to set a frame in which is no margin for interpretation. But the lawmaker could have stated examples in the recitals, that the work would be easier in the start.

The law does further not specify what the needed information to be provided are, to get a seal. This legal uncertainty is unsatisfying for processors and controllers. Especially because there is no minimum and no maximum on information which can be requested.

The open formulations also allow to amend the criteria over time, which can be hard for undertakings. In forms of higher cost and more managing effort.

The term of European Data Protection Seal is thrown up, but the law states not more than it is a common certification with criteria approved by the Board. Such a common seal, which is

[93] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196).

there to hinder national fragmentation is from high importance for the cross boarder data flow and the common market. The GDPR provides no further and with that not enough information about it.

The biggest advantage is that certificates have now a legal basis but are still voluntary, maybe the pressure created in the way that some cloud-service providers use them combined with the choice of the consumer will force all providers to use certificates.

Clearly would one argue even if a provider does not have a certificate he has to comply with the law, but he does not allow a third party to test and check his hard- and software in certain time intervals voluntarily.

Codes of conduct, like the certification, allow data subjects to quickly assess the level of data protection.

The codes of conduct can improve the standards by establishing a best practice and improve transparency and accountability, by giving data subjects a possibility to distinguish the organizations that meet the requirements of the law and that they can trust them with their personal data. Signing up for a code of conduct would mean constant monitoring for a undertaking and maybe compensation payments, suspension and exclusion from the code. But it could also be possible that the codes of conduct are not expanding data protection and undertakings would just agree on codes of conduct, containing the standard set down in the GDPR. There would be no additional value on data protection.[94]

In both constructs the information gaps in the awarding process must be closed.

Both measures are easy ways for controllers and data subjects to find out who can be trusted with data even though it is an extra burden to stay in the scope of the code or the certifications.

Controllers can fulfill their duties faster and easier than under the DPD. The constructs of codes of conduct and certification are a major improvement in the GDPR and a good step into the digital society, but are probably not going far enough by making certificates mandatory.

The right of control, selection and the decisional authority do not essentially change. The controller must select a processor which provides adequate safeguards and acts conform with the law. But through the higher data protection standard under the GDPR can be concluded that also the control must be conducted more detailed than under the DPD.

[94] Paal, in Paal/Pauly Datenschutz-Grundverordnung Kompaktkommentar,(2016), p.506

It is still not stipulated how often the controller needs to control the processor. The GDPR stays vague on this point.

Through the shift in the responsibilities and with that liability undertakings have to make sure that they have fast managing structures to quickly notify the controller in case of a data protection breach. This imposes higher costs for the undertaking but provides the end-user with higher transparency and enhances trust.

Summing up complying with the GDPR does demands higher costs and organizational burdens on the controller and processor. The relation between both gets more regulated by law than just by contract, this could mean financial losses for controllers and processors. The GDPR stipulates a more precautionary approach than the DPD, which means higher protection for the end-user which can be seen on the point of the relation between controller and processor as process.

4 Relation between processor and sub-processor

The systematically next step is to show the relation betwen processor and sub-processor before getting to the relation of controller and sub-processor.

4.1 Relation between processor and sub-processor under the DPD

This relation is a legal loophole under the DPD and is lacking on legislation. This becomes clear when considering the following points.

4.1.1 In general

Art.16,17DPD does not hinder the usage of sub-processors. But clearly states that processing must be done in accordance with the instructions of the controller or the requirements of the applicable law.[95] The Directive does not provide clear requirements for the appointment of sub-processors or if they fall under the scope or not.[96]

The later announced e-privacy Directive, from 2002, states in rec.32: "*Where the provider of an electronic communications service or of a value added service subcontracts the processing of personal data necessary for the provision of these services to another entity, such*

[95] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU.

[96] Gabel/Hickman, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU`s new data protection law,(2016), chap. 11.

subcontracting and subsequent data processing should be in full compliance with the requirements regarding controllers and processors of personal data as set out in the DPD".[97]

The e-privacy Directive does manifest that sub-processing falls under the scope of the DPD.

The later Commission Decision, to which was referred by the Art.29 Working Party[98], clearly states that: in contracts between processors and sub-processors it should be implemented that sub-processors must provide at least the same level of privacy and data protection, that the data controller provides and that processors can only engage sub-processors with the consent of the controller.[99]

In addition sub-processors can be liable to data subjects for damage claims, where it is not possible to bring a claim against the controller or processor. In such a claim sub-processors are only liable for their own activities.[100]

4.1.2 Contract

The engagement of sub-processors in cloud-computing can lead to a complex multitudinous construct. To assure the security of the data, the contractual requirements between processor and sub-processor stay the same as between the controller and the processor.[101]

The processor has to be sure to act within the consent, of the controller or the other justifications in Art.7DPD.

The consent can be given in the contract between controller and processor, within the terms and conditions. If not the processor can only engage sub-processors if he acts on the controllers behalf.

In cloud-computing cases where the main advantages are flexibility, fast scalability and cost efficiency, such clauses likely to appear in every contract.[102]

---

97 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

98 Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.13.

99 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU, §11.

100 Paez, New Standard Contractual Clauses for Data Transfers Out of the European Union Raise Concerns, (2010).

101 Eckardt/Hilber/Giebichenstein/Niemann/Helbig/Weiss, LeitfadenLeitfaden Cloud Computing, Recht Datenschutz & Compliance,(2010), p.16.

102 Brennscheidt, Cloud Computing und Datenschutz, (2013) p.122.

4.1.3 Liability

The controller is responsible for all actions of the processor and therefore the only party, who is liable Art.6DPD.[103] This means that the controller is also responsible for all sup-processors engaged by the processor. This comes from the contractual consent given in the contract between controller and processor without that consent the processor would not even be allowed to engage sub-processors. Art.29 Working Party states that for the case of infringements the controller should have contractual safeguards against the sub-processor and or processor.[104]

It can also be derivated from Art.23DPD which foresees only the controller to be claimable.

4.2 Relation between processor and sub-processor under the GDPR

Even though the GDPR does not define sub-processor it does contain similar obligations over sub-processors as the Commission Decision[105] which amends the DPD.

4.2.1 Contract

The processor shall only engage a sub-processor with prior written authorization specific or in general by the controller. Also does the processor need to notify the controller to give him time to intercept, when engaging an other processor, Art.28(2)GDPR.[106]

Art.28(9)GDPR read together with Art.28(4)GDPR states that the contract between the processor and the sub-processor must be in writing, including the electronic form.

Why the prior authorization must be in written form and the later agreed contract can only be in electronic form is not comprehensible. The later concluded contract does expose the data

[103] Grant/Lambert/Pickering, Data Protection Day - data processors and the GDPR,(2016).
[104] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), sec. 2.4.2.
[105] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU.
[106] The contractual relation follows the prior under the DPD announced, *2010/87/EU: Commission Decision 2010/87/EU: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council,* especially the right to intercept in the selection process of sub-processors was already addressed there,Art.11.

and the data subject to a higher risk than a prior authorization In argumentum e contrario it must be assumed that the electronic form is sufficient for the authorization[107]

The contract between processor and sub-processor needs to meet the same data protection obligations as the contract between the controller and the processor,Art.28(4),Art.28(3)GDPR. Especially the processor shall ensure that the sub-processor provides sufficient guarantees to implement technical and organizational measures to ensure compliance with the GDPR.

4.2.2 Right of control and selection

Under the GDPR it is not solely the processor to choose and select a sub-processor. The processor can under the formal requirements of consent engage another processor, which provides adequate safeguards and organizational measures to comply with the GDPR.

The processor must choose the sub-processor in the same way the controller chooses the processor, Art.28(4)GDPR. Processor and sub-processor must bind themselves in the contract between themselves to all the mandatory contractual content in Art.28(3)GDPR. With that is the burden of control solely on the processor.

Art.28(2)GDPR further differs two forms of authorization, the prior specific authorization and the general written authorization

In the case of the general written authorization the processor needs, when selecting a sub-processor to give the controller a notice and give him the opportunity to object, Art.28(2)GDPR, giving the controller a kind of veto right for the selection process.

Prior specific consent can only be understood in the way that the processor needs to ask the controller before engaging a sub-processor so that the controller can withdraw his consent.[108]

In consequence both forms of authorization are the same. But in the majority of cloud-computing cases the form of general written consent appears to be[109] more convenient for the cloud provider. He does not need to ask for consent every time. He just informs the controller and set a deadline in which the controller can object.

[107] Plath, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition,(2016), p.1135.
[108] Plath, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition,(2016), p.1136.
[109] Which I stated early must also be allowed in electronic form, argumentum e contrario, if the contract can be in electronic form.

4.2.3 Decisional authority and liability

The decisional authority of the processor over the sub-processor under the GDPR as well as under the DPD, strongly relates with the relation of the controller to the sub-processor.

The execution of the decisional authority will become clear when I discuss the relation between controller and sub-processor.

The processor remains fully liable to the controller for the performance of the sub-processors, Art.28(4)GDPR.[110]

4.3 Comparison of the relation between processor and sub-processor under the DPD and the GDPR

The formal requirement, specificity the contractual minimum content, between processor and sub-processor under the GDPR is higher, than under the DPD. The GDPR provides clear requirements and is easier accessible for everyone, than the Opinion of the Art.29 Working Party[111] of the DPD, which is also not binding. The contractual minimum criteria are now legally binding implemented.

The legal loopholes under the DPD which the Commission Decision closed by amending the contractual standard clauses do not occur with wider scope and the provisions in Art.28(2), (4)GDPR under the Regulation.

For cloud-computing especially the possibility to object is the best what could happen to an end-consumer. As stated above the end-consumer is the controller in cloud computing cases, this allows the "small" end-user to reduce the number of entities involved and with that the likeliness of personal data breaches to appear.

This could dramatically hamper the efficiency and flexibility of cloud-computing.

The big change of liability does also manifest here, the processor is liable for the actions of the sub-processor, which obliges the processor to sufficiently make sure the sub-processor is complying with the law and to execute rights of control properly.

[110] Heywood, Obligations on data processors under the GDPR,(2016).
[111] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), 2.4.2.

5 Relation between controller and sub-processor

5.1 Relation between controller and sub-processor under the DPD

Between the client and the sub-contractor the DPD does not establish a direct relation.

From that arises the discussion if rights against the sub-processors exist and how they are executed.

5.1.1 Selection, decisional authority and right of control of controllers over sub-processors

It is controversial if the controller has a right to influence the choice of sub-processors or has a right to control sub-processors.[112]

It is partly represented that the controller has the obligation to make sure the choice is made thoroughly[113] or to give criteria to the processor how to choose sub-processors.[114]

Under the DPD the discussion leads to three though models how the rights could be executed.

Those models are: the model of through-reaching controller rights, the stage model and the model of several clients.

5.1.1.1 Model of through-reaching controller rights

The keynote in this model is that the controller is the central figure of processing and every other entity is just a helping one.

The controller can directly use his rights against the sub-processor. The right of control and the decisional authority is used directly against the subcontractor. The processor, in the middle, will be left out of this relationship.[115]

The DPD does not determine, if the controller should have own authority over the subcontractor or not, Art.17DPD.[116] But also does the DPD itself not distinguish between processors and sub-processors.

---

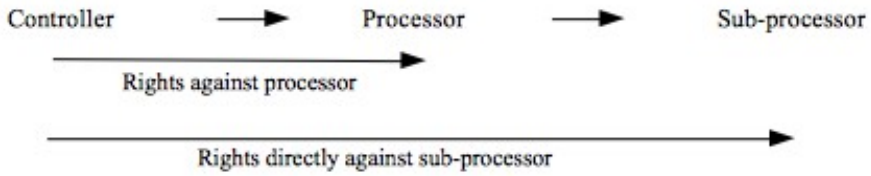
[112] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.266ff..

[113] Gabel, in Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG(2013)§11.

[114] Kremer, (Unter-)Unterauftragnehmern nach dem BDSG“, in ITRB(2014), p.60(64).

[115] Bogners/Krupna, Der Subauftragnehmer im Rahmen der Auftragsdatenverarbeitung – Weisungs- und Kontrollrechte in einer Auftragskette, in RDV(2014), p.19-25.

[116] Becker, Auftragsdatenverarbeitung: Weisungs- und Kontrollrechte im Unterauftragsverhältnis,(2015).



For cloud-computing cases this would mean that the processor engages a sub-processor to execute his business by supporting him with a service, while the controller needs to control the sub-processor.[117] This can become very expensive for the controller, keeping in mind the high number of processors and sub-processors involved in regular cloud-computing scenarios.[118]

5.1.1.2 Stage model

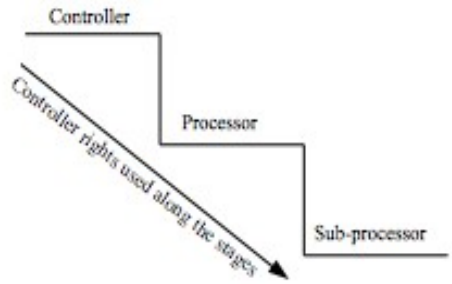
In this model the controller, the processor and the sub-processor are on different stages, a hierarchy.

The controller gives orders to the processor which hands them down to the sub-processor, an authority and control right used along the stages.

There is no direct relation between the controller and the sub-processor. The controller rights have no direct application against the sub-processor. The controller can only execute its rights against the processor and the processor can only execute his against the sub-processor. Along the stages the controller stays data proprietor.[119]

The processor has own decisional authority over the sub-processor but only inside the opened frame of maneuver by the controller.

The liability in such cases can vary and depend on contractual relations between the parties.



The stage model does also appear in the form of a stage model with modified obligations.

[117] Brennscheidt, Cloud Computing und Datenschutz,(2013) p.127.
[118] Hartung/Storm, in Hilber Handbuch Cloud Computing,(2014), p.362.
[119] Becker, Auftragsdatenverarbeitung: Weisungs- und Kontrollrechte im Unterauftragsverhältnis,(2015).

In a cloud computing case this would mean that the user, as controller, gives instructions to the cloud provider, as processor, who forwards them to the sub-processors. The controller is liable and responsible for all parties in this hierarchy. This weakens the protection of the average users who do not know about their duties[120] and responsibilities or even their liability.

5.1.1.2.1 Stage model with modified obligations

The theory of the stage model with modified obligation combines the stage model with the model of through-reaching controller rights. The rights of the controller are used along the stages but the controller has the duty to inform himself that the rights of selection and control are properly executed by the processor (modified obligation).[121]

Those obligations can easily be fulfilled in the way that the processor shows the documentation, certification of control over the sub-processors to the controller. Those obligations must, under the DPD, necessarily be in a contract to clearly determine what reach those obligations have.

The theory does also leave room for the direct right of access in the case of a breach of trust. It can be implemented in the contract between the parties

5.1.1.2.2 Direct right of control in the case of a breach of trust

Especially in the stage model compared to the other two models it is controversial if the controller has got a direct right of control against the sub-processor when the duty of control is not properly conducted by the processor.[122]

There is no legal backing for such a right in the DPD but a practical need. The controller or cloud-user can not longer trust the information provided by the processor and a direct right of control for such cases, like in in the model of through-reaching controller rights is probably the only way to get things straight out of the view of the controller.[123]

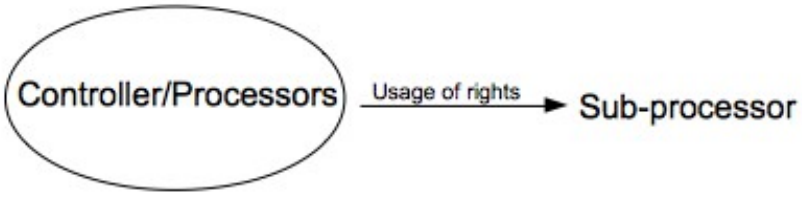
Such a right must be manifested in the contract between the parties. This modification of the stage model tries to satisfy in regard of the fact that only the controller can be held liable under the DPD.

---

120 Duties of control and selection.
121 Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.262ff..
122 Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.263f..
123 Bogners/Krupna, Der Subauftragnehmer im Rahmen der Auftragsdatenverarbeitung – Weisungs- und Kontrollrechte in einer Auftragskette, in RDV(2014),p.19-25.

5.1.1.3 Model of several clients

This model is a hybrid form of the two above. The sub-processor is under the decisional authority of the controller and the processor, he has to follow the instruction of both. The case of disintegrating instructions should not appear, because the processor can only instruct the sub-processor in the way he is instructed himself by the controller.[124]



5.1.1.4 Model under the DPD

All models are thought experiments but nevertheless important for the understanding of the execution of rights and the relation of the parties in cloud-computing cases.

The model of several clients does prima facie appear to be easy but is de facto the most difficult one to implement. It comes with high burdens to the contract, which should clearly state that this model is used. Out of transparency reasons every decisional authority would be needed to be named in the contract. Especially this is difficult in up to three-digit sub-processor chains. A change of only one sub-processor would need huge contractual amendments.[125] But also this model can be helpful in individual cases.
The model of several clients is a minority opinion because it denies the legal figure of processing and sub-processing, by acting against factual relations between controller and sub-processor. This is undermining the basic efficiency thought, by not providing a own frame of maneuver to the processor, which is one of the biggest advantages of cloud-computing.[126]

Arguments against the model of through-reaching controller rights can be hold that it is impractical, because it comes with strong relations between the controller and the sub-processor, which are atypical for the nature of cloud-computing. Those two parties usually do not interact with each other.

In addition the model of through-reaching controller rights does leave out the processor in the whole relation. But it is the processor who engages the sub-processor.[127]

[124] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.262ff..
[125] Becker, Auftragsdatenverarbeitung: Weisungs- und Kontrollrechte im Unterauftragsverhältnis,(2015).
[126] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.262ff..
[127] Herold, Unterschätzen Sie niemals das Unterauftragsverhältnis in der Auftragsdatenverarbeitung,(2015).

The ruling opinion in the literature is the one of the stage model, in individual cases with modifications. De facto it satisfies the nature of cloud-computing and processing the most.[128]

Compared to the model of through-reaching controller rights the processor is not left behind and can still use own control rights and decisional authority.

The controller in the stage model must implement three organizational measures: (a) make sure processors and all sub-processors are controlled, (b) all processors are obliged to control those engaged subcontractors, (c) they all have to inform themselves if the control is properly made.[129]

Only if these three points are addressed in the contract between all three parties the stage-model can properly function

Because no model stems from the law these three points must be met in the contracts between the parties.

Especially the stage model ensures the advantages of cloud-computing of fast flexibility and efficiency and guarantees every party a frame of maneuver.

The Art.29 Working Party itself prefers the usage of a stages model with only two stages.[130] In this model is only one controller and one or several processors which have to follow the controllers instructions. Sub-processing would not occur.

In cases with controllers, processors and sub-processors the Working Party states:"*the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities*."[131]

This sentence allows the interpretation of a stage model, which is established by contracts or a more precise on the wording of the law interpretation of the model of through-reaching controller rights.

I conclude that the Art.29 Working Party prefers in complex cloud-computing structures the usage of the model of through-reaching controller rights, because of the following reasons.

The arguments of the Art.29 Working Party for the model of trough-reaching rights, against the stage model are, that it meets the requirements of liability better than the ruling opinion in

[128] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.263.
[129] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.263.
[130] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9.
[131] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9.

the literature and the rights are executed effectively. In the stage model is the liability often determined by the contracts between the parties.[132]

Further stand for the through-reaching model the argument that the law differs only between two fractions: processors and controllers. When the processor controls a sub-processor he is kind of self controlling.[133]
In addition stands against the model of through-reaching controller rights that a comprehensive control right of the sub-processor through the controller is not designated in the DPD. There is no need for a double right: (a) from the controller against the sub-processor and (b) from the processor, against the sub-processor.[134]

Conducting the rights double would be inefficient and would throw up difficult questions of the relation between the right of selection and the right of control. The assumption of a stage skiping right (through reaching controller rights) lacking of practical relevance and brings with it a high organizational burden.

Continuing a control in person of the sub-processor through the controller at all servers would be nearly impossible, the only ways to check is to use third persons or certificates. The bigger the chain of subcontractors is, the bigger becomes the risk of data infringements for the controller and enforcing rights becomes more difficult. The literature further demands to limit the length of the chain of subcontractors, to enhance data-privacy right protection and minimize risk of breaches.[135]

Also does the Art.29 Working Party acknowledge that the stage model can function properly, but only when the contracts between the parties contain a consent clause in regard of sub-contracting and the possibility for the controller to object in the choice of sub-processors.[136]

In case of doubt should the model of through-reaching controller rights be used, because it is closer to the wording of the law.[137]

There are many arguments against the model of through-reaching controller rights, but they can not convince. The point of liability is the one which satisfies the usage of the through-reaching controller rights. It clearly allocates the risks of cloud-computing by meeting the

[132] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9.
[133] Brennscheidt, Cloud Computing und Datenschutz,(2013) p.127.
[134] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.269.
[135] Niemann/Hennrich, Kontrolle in den Wolken?, in CR(2010), p. 686(692).
[136] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9f..
[137] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9f..

wording of the law the best, which determines in the DPD that only the controller is liable. There is no gap for interpretation on the point of controller`s liability. The stage model, also in the form of the stage model with modified obligations and with a direct right of control for the case of a breach of trust, can not be preferred. Because of the liability character it is in the interest of the controller to have direct rights against the sub-processor.

5.2 Relation between controller and sub-processor under the GDPR

As under the DPD is the relation between controller/cloud-user and sub-processor not explicitly regulated. There is usually no contractual relation between the cloud-user and the sub-processor.

5.2.1 Rights of: selection, decisional authority and of control

The controller does not solely have a right to select sub-processor, it is the processor who engages the sub-processor, Art.28(4)GDPR, but with concessions to the controller. The law allows varying interpretations in which execution model the rights will be executed. By identifying the model I can also describe the rights itself.

5.2.2 Model execution under the GDPR

It is still open which model will be used under the GDPR and the practice will show, which one is best.

In my eyes there are only two models which come to mind. The one from the Art.29 Working Party preferred through-reaching controller rights model and the by the literature favored stage model.

The model of several clients stays under the GDPR as under the DPD a model with a small scope of application. It can be the best option in certain cases but is not representative for the majority of cases, because of the reasons stated above, like: a high contractual burden, which especially in cloud-computing cases with standardized contractual terms makes it hard to amend the contracts if a party changes.

For the stage model stand the arguments of Art.28(2)(Sentence:1)GDPR "*The processor shall not engage another processor without prior specific or general written authorization of the*

controller" ,as under the DPD, the processor can only act under the instruction and within the consent of the controller. Further is in Art.28(4)GDPR the wording "on behalf of the controller" the processor engages a sub-processor on the instruction of the controller. Concluding that: it is the processor who engages the sub-processor and who is responsible for the contractual negotiation. This manifests a hierarchy.

Continuing the understanding and interpretation of Art.28(4)GDPR is split. The wording:

"where a processor engages another processor[...] the same data protection obligations as set out in the contract[...] between the controller and the processor [...] shall be imposed on that other processor by way of a contract[...]" could be understood in the way that the processor becomes controller over the sub-processor and has to act like a controller over it.

This would mean that the primal controller has no direct decisional authority over the sub-processor. The controller can only instruct the processor which itself can instruct, with contractual rights like a controller, the sub-processor.

Art.28(2)(Sentence:2)GDPR obliges the processor to inform the controller if a sub-processor is engaged or changed and allows the controller to object. This objection right manifests the stage model in the way that the processor can choose but only in the "frame of maneuver" given by the controller.

For the model of through-reaching controller rights the arguments are hold that

The fact that the GDPR does not differ in the wording between sub-processor and processor and just titles them as "processor" and "processes engaged by another processor". This allows the interpretation that all processors are on the same stage in the hierarchy under the controller. With that would all the obligations on processors also apply to sub-processors.

A different interpretation of Art.28(4)GDPR is that: the wording:
"where a processor engages another processor[...] the same data protection obligations as set out in the contract[...] between the controller and the processor [...] shall be imposed on that other processor by way of a contract[...]"
shall also allow the interpretation that the processor must take care that the sub-processor must directly obey the orders of the primal controller, as Art.28(3)(a)GDPR states: "*processes the personal data only on documented instruction from the controller"*.
This allows a direct execution of the decisional authority from the controller against the sub-processor.

The Art.29 Working Party wanted, under the DPD in complex structures, a clear allocating of risks and authority.[138]

But under the GDPR is the allocation of risks determined by the law. Under the GDPR it is not only the controller, who is liable, but also the processor, who is liable for own actions and liable for the actions of the engaged sub-processors, Art.28(4)GDPR.

The argument of allocation of risks is obsolete.

Despite that the stage model still contains a dispersing character.

Against the model of through-reaching controller rights stand the same arguments, as under the DPD shown above.

The split interpretation of Art.28(4)GDPR can be decided.

When assuming that Art.28(4)GDPR must be interpret in the way that the controller can directly execute its rights against the sub-processor. The Processor would not be involved.

The difference under the GDPR is that the processor is liable for the actions of the sub-processor, Art.28(4)GDPR.

This would mean that the controller could directly instruct the sub-processor, the processor would be liable for the sub-processors actions, but could not give instructions to the sub-processor. Such an outcome is unbearable.

In cloud-computing cases, which demand high flexibility, a controller as central figure does not satisfy the cloud-computing nature. It is hard to imagine that a single controller can instruct every single processor and sub-processor by own. This would demand an immense cost and time effort, which not every undertaking or natural person could afford.

Both models do not completely satisfy the needs of cloud-computing. The stage model still has the problem of dispersing the order along the stages as well as the model of through-reaching controller rights lacks on flexibility and efficiency.

But in my eyes do the clear contractual rights, which have to be guaranteed in Art.28(4)(3)(a)-(h)GDPR mitigate the dispersing character of the stage model.

[138] "the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities.", Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196), p.9f...

The stage model satisfies the most because every party is only liable for the one it has decisional authority over and the duty to control and select. Also does the stage model satisfy the advantages of cloud-computing the best.

Continuing it could be that under the GDPR the stage model is modified with obligations or does contain a direct right of control for the case of a breach of thrust.

The initial thought behind both models was to meet the fact that only the controller is liable and to satisfy the need of the controller to have a ultima ratio right for a worst case scenario.

This argument is obsolete under the GDPR with the liability of the processor for the sub-processor and the contractual minimum standard in Art.28(4)(3)(a)-(h)GDPR.

The contractual minimum content established a kind of upside down modified obligation in the stage model, in comparison to the modified obligation under the stage model under the DPD, for. e.g.: is the sub-processor obliged to help the controller carrying out his obligations, Art.28(4)(f)GDPR, returns all the personal data to the controller after the end of the provision, Art.28(4)(g)GDPR and especially Art.28(4)(h)GDPR make available to the controller all information necessary to demonstrate compliance.

The sub-processor is obliged to meet certain requirements in the relation controller, sub-processor. It is not the controller who is executing directly against the sub-processor.Direct rights between controllers and sub-processors do not exist. The rights are used along the stages, but the sub-processor must fulfill duties in relation to the controller.

5.2.3 Liability

The controller is not liable for the sub-processor the law clearly states in Art.28(4)GDPR that the processor is liable to the controller for the actions of the sub-processor. The data subject has jurisdictional remedies against every party, not only controllers, which infringed its rights, Art.79GDPR.

5.3 Statement to right execution models under both frameworks

The shift from the through-reaching model to the stage model manifests a win-win situation for controllers and processors as well as for data-subjects.

Under the GDPR with the contractual minimum criteria for the contract, the stage-model became mandatory by law.

The efficiency character and the own room of maneuver for processors and "sub-processors" as well as the allocation of liability convinces. This is only possible through the implementation of liability and obligations on processors. The stage model, the ruling opinion in the literature under the DPD[139] satisfies most the character of cloud-computing,: efficiency, scalability and economically, and unleashes the power of cloud-computing.

The GDPR provides clear, easy to follow rules and provides data-subjects with rights against the party, who actually breached their rights.

6 Conclusion

I compared and discussed the relation of controller, processors and sub-processors under both frameworks in every constellation.

The question, if the legal relation between the parties in cloud-computing or in general in processing activities constitutes a progress in the digital age is going to be answered here.

Some argued that the GDPR will kill the cloud by over regulating it and making it only possible for big entities to follow the rules.[140] This would tend that the GDPR would mean a stagnation or regression for the concept of clouds.

Data protection law is strongly influenced by the EU bodies. From the first drafts of definitions of processors and controllers shaped during the negotiation of the Convention 108[141] in 1981, over the DPD in 1995 over the Commission Decision[142] in 2010, over the Art.29 Working Party opinion on cloud-computing[143] in 2012 to the GDPR, which will enter into force in 2018, a clear trend was recognizable.

The system shifted from a model with only one liable party to a more fair model with processors and controller nearly equally liable. This will not kill the cloud, it is just a reaction to establish a model with a fair distribution of risks. The fair distribution of risks constitutes progress.

The GDPR in the light of the digital age is a step in the right direction. The regulation constitutes a major step for the individual data right protection by providing more rights with

[139] Borges/Meents, Cloud Computing Rechtshandbuch,(2016), p.263ff..
[140] Hon, GDPR: Killing cloud quickly?,(2016).
[141] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108.
[142] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU.
[143] Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing(01037/12/EN WP 196)

a bigger scope. In addition does the GDPR by picking up known concepts from the past and amending them in a way that even border cases like cloud-computing can properly be addressed in the future constitute progress.

Taking all this into account it is clear that the GDPR constitutes progress in the digital age.

Table of reference

List of Judgments/Decisions:

- ECJ, C-101/01, Bodil Lindqvist, 06.11.2003
- ECJ, C-131/12, Google vs. Spain, 13.05.2014

Treaties/Statutes/Law text/Recommendations/Commission Decisions:

- Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (00264/10/EN WP 169)
- Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing (01037/12/EN WP 196)
- Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010/87/EU.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108
- European Data Protection Supervisor, Q&A 10) Cloud Computing https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA10
- 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
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Memo of the European Commission, Unleashing the Potential of Cloud Computing in Europe - What is it and what does it mean for me?, (27.09.2012)
- Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93
- 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)

- Bundesdatenschutzgesetz (BDSG), (2003)

Literature:

- Abu-rab Sufian, Baun Christian, Kunze Marcel, Kostenvergleich: Cloud Computing vs. Hosting-Cotangent, in iX (12/2011), p.126-130
- Becker Tim, Auftragsdatenverarbeitung: Weisungs- und Kontrollrechte im Unterauftragsverhältnis, (2015), https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-weisungs-und-kontrollrechte-im-unterauftragsverhaeltnis/, (last visited: 24.11.2016)
- Bedner Mark, Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung, (2013)
- Bergmann Lutz/Möhrle Roland/Herb Armin, Datenschutzrecht Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz, (2016)
- Bird&Bird, GDPR – Timeline, http://www.twobirds.com/en/practice-areas/privacy-and-data-protection/eu-framework-revision, (last visited: 24.11.2016)
- Bogners Frank/Krupna Karsten, Der Subauftragnehmer im Rahmen der Auftragsdatenverarbeitung – Weisungs- und Kontrollrechte in einer Auftragskette, in RDV (2014),p.19-25.
- Borges Georg/Brennscheid Kirstin, in Borges/Schwenks Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, (2012)
- Borges Georg/Meents Jan, Cloud Computing Rechtshandbuch, (2016)
- Bracy Jedidiah, Article 29 Working Party lays out GDPR action plan, (2016), https://iapp.org/news/a/article-29-working-party-lays-out-gdpr-action-plan/, (last visited: 18.11.2016)
- Brennscheidt Kirstin, Cloud Computing und Datenschutz, (2013)
- Computerweekly.com, SaaS remains most popular form of cloud computing for UK IT (2013).
- Datenschutz Praxis, Wichtige Datenschutz-Begriffe, Was genau versteht man unter Funktionsübertragung? Externe Dienstleister und Datenschutz, (2015), https://www.-

datenschutzbeauftragter-info.de/externe-dienstleister-und-datenschutz/, (last visited: 16.11.2016)
- Eckardt Jens/Hilber Marc/Giebichenstein Rüdiger/Niemann Fabian/Helbig Thomas/Weiss Andreas, Leitfaden Cloud Computing, Recht Datenschutz & Compliance, (2010)
- De Hert Paul/ Czerniawski Michal, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, (2016)
- Der Landesbeauftragte für den Datenschutz Baden-Württemberg, Auftragsdatenverarbeitung und Funktionsübertragung, (2012)
- Frampton Katie, The difference between IaaS, SaaS and PaaS, (2013), https://www.smartfile.com/blog/the-differences-between-iaas-saas-and-paas/, (last visited: 24.11.2016)
- Gabel Detlev, in Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, (2013)
- Gabel Jürgen/Hickman Tim, Unlocking the EU General Data Protection Regulation: A practical handbook on the EU`s new data protection law, (2016)
- Geis Ralf, Ein Rahmenwerk für den elektronischen Rechtsverkehr: Zugleich ein Beitrag zur Modernisierung gerichtlicher Verfahren dargestellt am Beispiel der Verwaltungsgerichtsbarkeit Rheinland-Pfalz, (2014)
- Gilbert Francoise, EU General Data Protection Regulation: What Impact for Businesses Established Outside the EU, (2016), http://www.lexology.com/library/detail.aspx?g=ebc6f7e5-ea46-43f3-92f3-db0fba6a9a12, (last visited: 11.10.2016)
- Gottlieb Cleary, The General Data Protection Regulation: Key Changes and Implications, (2016), https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201650.pdf, (last visited: 24.11.2016)
- Grant Hazel/Lambert Amy/Pickering Kate, Data Protection Day - data processors and the GDPR, (2016), http://www.fieldfisher.com/publications/2016/02/data-protection-day-data-processors-and-the-gdpr#sthash.tIsv9vXy.dpbs, (last visited: 24.11.2016)
- Gutwirth Serge, Leenes Ronald, De Hert Paul, Data Protection on the Move: Current Developments in ICT and Privacy/Data, (2016)

- Hamdaqa Mohammad/Tahvildari Ladan, Cloud Computing Uncovered: A Research Landscape, in Advances in Computers, (2012), vol.86, p.41-85
- Haupt Michael, "Data is the New Oil"—A Ludicrous Proposition Natural resources, the question of ownership and the reality of Big Data, (2016), https://medium.com/twenty-one-hundred/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294#.awcz3r65y, (last visited: 24.11.2016)
- Hartung Jürgen/Storm Nicholas, in Hilber Handbuch Cloud Computing, (2014)
- Heidrich Joerg/Wegener Christoph, Sichere Datenwolken – Cloud Computing und Datenschutz, in MMR (2010), p.803
- Heimes Rita, Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/, (last visited: 16.11.2016)
- Herold Philipp, Unterschätzen Sie niemals das Unterauftragsverhältnis in der Auftragsdatenverarbeitung, (2015), https://www.mein-datenschutzbeauftragter.de/blog/20150521-unterschaetzen-niemals-unterauftragsverhaeltnis-in-auftragsdatenverarbeitung/, (last visited: 16.11.2016)
- Heywood Debbie, Obligations on data processors under the GDPR, (2016), https://united-kingdom.taylorwessing.com/globaldatahub/article-obligations-on-data-processors-under-gdpr.html, (last visited: 16.11.2016)
- Hon Kuan, GDPR: Killing cloud quickly?, (2016), https://iapp.org/news/a/gdpr-killing-cloud-quickly/, (last visited: 16.11.2016)
- Hon Kuan/Millad Christopher/Walden Ian, Negotiating cloud contracts: Looking at clouds from both sides now, in Stanford Technology Law Review, Vol.16 (1/2012)
- Honbo Zhou, The Internet of Things in the Cloud: A Middleware Perspective, (2012)
- Höllwarth Tobias, Cloud Migration, (2011)
- Hustinx Peter, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, (2013)
- Jotzo Florian, Der Schutz personenbezogener Daten in der Cloud, (2013)
- Kian Bardia, Cloud Computing - Herausforderung für das Rechtssystem, (2016)
- Kremer Sascha, (Unter-)Unterauftragnehmern nach dem BDSG", in ITRB (2014), p.60

- Meissner Sebastian, Zertifizierungskriterien für das Datenschutz Gütesiegel EuroPriSe, in DuD (2008), p.525
- Michel Johannes, Datensicherheit und Datenschutz im Cloud Computing. Fallstudie und kritische Analyse, 2.4.1ff., (2013)
- Niemann Fabian/Hennrich Thosten, Kontrolle in den Wolken?, in CR (2010), p. 686
- Oxford Dictionary of English, (2010)
- Paal Boris, in Paal/Pauly Datenschutz-Grundverordnung Kompaktkommentar, (2016)
- Pachghare, V.k., Cloud computing, (2015)
- Paez Mauricio, New Standard Contractual Clauses for Data Transfers Out of the European Union Raise Concerns, (2010), http://www.jonesday.com/new_standard_contractual_clauses/#_edn4, (last visited: 20.11.2016)
- Petri Thomas, in Smitis Kommentar Bundesdatenschutzgesetz, 8.edition, (2014)
- Plath Kai-Uwe, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition, (2016)
- Steinle Thomas, Auftragsdatenverarbeitung bs. Funktionsübertragung – Teil 2: Unterscheidungskriterien, (2012), http://www.it-rechtsanwalt.com/datenschutz/auftragsdatenverarbeitung-vs-funktionsuebertragung-teil-2-unterscheidungskriterien-3377.php, (last visited: 20.11.2016)
- Stitilis Darius; Malinauskaite, Compliance with basic principles of data protection in cloud computing: the aspect of contractual relations with end-users, in European Journal of Law and Technology, vol.5, nbr.1, (2014)
- Stumper Kai, Abgrenzung Auftragsdatenverarbeitung – Funktionsübertragung, (2014), http://www.firstlex.de/abgrenzung-auftragsdatenverarbeitung-funktionsuebertragung-_913/, (last visited: 20.11.2016)
- Von Braunmühl Patrick, in Plath Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. edition, (2016)