Consent now and then

University: Tilburg University
Master: Law & Technology
Author: D.C.J. van Casteren
ANR: 524830
Studentnumber: 1266169
First supervisor: mr. C. Quelle
Second supervisor: mr. drs. B. van der Sloot

Tilburg, 5 June 2017

Consent now and then

University:	**Tilburg University**
Master:	**Law & Technology**
Author:	**D.C.J. van Casteren**
ANR:	**524830**
Studentnumber:	**1266169**
First supervisor:	**mr. C. Quelle**
Second supervisor:	**mr. drs. B. van der Sloot**

Tilburg, 5 June 2017

Table of contents

List of abbreviations

Art.	Article
CJEU	Court of Justice of the European Union
CoE	Council of Europe
Commission	European Commission
DPD	Data Protection Directive
EC	European Commission
ECHR	European Convention on Human Rights
Et al.	And others
Etc.	And so on
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
Rec.	Recital
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom of Great Britain and Northern Ireland
US	United States of America
Working Party	Article 29 Working Party

1. Introduction

This thesis is about the right to privacy and data protection.[1] It will more specifically focus on the legal grounds that can be utilized to base the processing of personal data on, in particular the legal ground based on the consent of the individual whose personal data are being processed.

1.1 Data protection, the (new) legal framework and processing based on consent

In the EU the fundamental right to data protection is currently (among other international instruments) governed by the DPD[2] and its national implementations. This directive has been into force since 1995 and was adopted to bring EU member state law concerning data protection closer together.[3] In early 2012 however a replacement for the DPD was proposed by the EC. According to the commission new challenges to the protection of personal data have arisen, the reason being rapid technological developments and globalization.[4] The DPD has furthermore not prevented fragmentation of data protection, legal uncertainty and a widespread public perception that there are significant risks associated with online activity.[5] This is why the commission at the time deemed a new legal framework necessary. Now four years later the proposed legal framework has gone through the complete legislative process and is soon to become reality for the whole of the EU (and beyond); the GDPR[6] has come into force twenty days after its publication in the Official Journal of the European Union, the 25th of May 2016 to be exact. It will however not apply until the 25th of May 2018 according to the regulation.[7]

This new legal framework brings a lot of changes with it for data protection in the EU. First of all the choice of a regulation instead of a directive has big implications. Harmonization problems of the past should because of this disappear, although practice has to determine

[1] Art. 8 ECHR and art. 8 EU Charter, see also art. 16 TFEU.
[2] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[3] Rec. 3, 7 and 8 DPD.
[4] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final, p. 1-2.
[5] See note 4.
[6] 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).
[7] Art. 99(2) GDPR.

whether this is correct.[8] A second change is the addition of new rights for data subjects, an example of which is the right to be forgotten.[9] Following the CJEU Google Spain decision[10], this right entails the possibility for data subjects to in certain cases have their personal data erased. Another example is the right to data portability[11], which in certain cases gives data subjects the right to take their personal data from one controller to another controller. Other important changes entail new obligations for data controllers and processors which will improve the position of data subjects, such as the data breach notification[12], and the addition of data protection officers as mandatory positions for many data controllers and processors.[13] Finally, the framework reform brings changes to the rules on the lawful processing of personal data. One of the legal grounds for lawful processing of personal data that is changed is consent. Processing based on consent can be regarded as processing based on permission of the individual whose data are processed. Consent as a basis for processing has played an important role in conceptions of data protection and privacy.[14] In fact, most daily, ordinary processing activities surrounding us use consent as their legal basis.[15] Looking at the recitals of the GDPR, this status of importance of consent does not seem to have changed with the entry into force of the GDPR[16]. The use of consent in data protection law is however not uncontested.

1.2 Research problem; consent now and then

The use of consent as a basis for processing personal data is regarded as problematic, as it is not providing adequate data protection in online environments. Koops says that with internet-based services consent in many cases is largely theoretical, having no practical meaning as most people just agree with something they have not read or understood.[17] Schermer et al distinguish a number of practical reasons for this. First of all there is a 'consent transaction overload'. There are simply too many consent requests for individuals to consider, watering down the psychological effect of being confronted with a consent transaction.[18] Second of all there is an 'information overload', which means that individuals are presented with too much,

[8] De Hert & Papakonstantinou, *Computer Law & Security Review* 2016, p. 182.
[9] Art. 17 GDPR.
[10] CJEU C-131/12, 13 May 2014 (*Google spain*)
[11] Art. 20 GDPR.
[12] Art. 33 and 34 GDPR.
[13] Art. 37 GDPR.
[14] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 3-6.
[15] De Hert & Papakonstantinou, *Computer Law & Security Review* 2016, p. 187.
[16] See rec. 40 GDPR.
[17] Koops, *International Data Privacy Law* 2014, p. 3.
[18] Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16, p. 176-177.

often difficult and highly legalistic, information in consent transactions.[19] According to Hull in particular "free" websites like Facebook have every incentive to make privacy notices as vague possible, as their product is access to individuals who have entered personal information.[20]. Third of all, individuals do not really have a meaningful choice when given a consent request, and are left with a non-negotiable 'take it or leave it' scenario.[21] Koops mentions in this regard that there is no realistic alternative to this practice, as most other providers of services apply the same practices.[22] Moreover, relating to this absence of a meaningful choice, Hull writes that it will become increasingly difficult to resist information disclosure as more and more life moves online.[23] Hull mentions that Facebook (a social network site) for example has been tied to college students' social capital for years, and that asking a student to leave Facebook in favor of their privacy would have a high price.[24] Because of the three practical reasons mentioned before, Schermer et al speak of consent desensitization: users no longer make active, informed choices when confronted with a consent situation, but instead just choose to provide consent when asked for it.[25]

Solove goes deeper into the matter and states that the current idea of privacy self-management, with consent being the implementation of it, does not provide people with meaningful control over their data as a number of problems plague the notion of privacy self-management.[26] According to Solove, privacy self-management suffers from both cognitive problems, which concern challenges caused by the way humans make decisions, and structural problems, which are about challenges arising from how privacy decisions are designed.[27] Like Koops and Schermer et al wrote, one of the (cognitive) problems is that individuals are often uninformed because they do not read that which they are consenting to. A possible explanation for this according to Solove is that privacy notices are long and difficult to comprehend.[28] According to Solove there is also a more difficult problem with proposals for improved notices, as making notices simpler and easier to understand conflicts with fully informing individuals.[29]Another cognitive problem according to Solove is the

[19] Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16, p. 177.
[20] Hull, *Ethics Inf Technol* 2015/17, p. 91.
[21] Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16, p. 177-178.
[22] Koops, *International Data Privacy Law* 2014, p. 4.
[23] Hull, *Ethics Inf Technol* 2015/17, p. 94.
[24] See note 23.
[25] Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16, p. 178.
[26] Solove, *Harvard Law Review* 2013/1880, p. 1883.
[27] See note 26.
[28] See note 26.
[29] Solove, *Harvard Law Review* 2013/1880, p. 1885.

problem of skewed decision making. Even if individuals would read and understand privacy texts instead, they would lack the expertise to fully assess the privacy consequences of agreeing to these texts. This is because people have "bounded rationality", which means that they struggle to apply their knowledge in complex situations.[30] Yet even if individuals are both informed and rational, the system still faces structural problems according to Solove. A first problem is that there are too many entities collecting data, which can make the consent decisions impossible for individuals to handle.[31] A second problem is the problem of aggregation. Individuals struggle to assess how their data might be aggregated in the future.[32] The reason for this is that pieces of (regarded as meaningless) data which are given now could in the future be combined and reveal sensitive information.[33] A third problem relates to this problem. According to Solove, people have difficulty in assessing (future) harm. The reason for this is that privacy is a long term issue (as the aggregation problem made clear), whilst most decisions to consent are tied to short-term benefits.[34]

These aforementioned points make clear that the processing of personal data may be poorly based when consent is the path that is taken by the data controller or processor, and that given consent might not really portrait the individual's wishes. Moerel and Prins speak in this regard of a 'mechanical proceduralism', whereby data controllers notify individuals and ask for consent in a mechanical manner, without offering effective data protection.[35] According to them, consent is in many cases rendered meaningless because companies anticipate that people routinely give their consent.[36] Given the fact that consent was and still seems an important way of legitimizing the processing of personal data, these critiques are worrisome. The critiques mean that current data processing based on consent may be flawed. Instead of empowering individuals and granting them more control over their personal data, it may offer them very little control in practice as *individuals may just consent every now and then, without proper choice and/or thought.* Consent is however still present in the new GDPR. The continued use of consent thus raises a few questions. A first question is what the changes to

---

See also Koops, *International Data Privacy Law* 2014, p. 4 about this trade-off between meaningful and practical consent.

[30] Solove, *Harvard Law Review* 2013/1880, p. 1887.

[31] Solove, *Harvard Law Review* 2013/1880, p. 1888.

[32] Solove, *Harvard Law Review* 2013/1880, p. 1889.

[33] Solove, *University of Pennsylvania Law Review* 2006, Vol. 154, No. 3, p. 505.

[34] Solove, *Harvard Law Review* 2013/1880, p. 1891.
See also Acquisti & Grossklags. *IEEE Security & Privacy* 2005, p. 26 – 33.

[35] Moerel & Prins 2016, p. 8.

[36] Moerel & Prins 2016, p. 48.

consent mean and if they justify the continued use of consent. Another question it raises is why we attribute consent such a prominent role as a means for legitimizing data processing that we insist on still using it. This research will as a result be about consent-based data processing. It will describe the current and upcoming legal rules regarding consent in European Union data protection law, as well as the reasoning behind the changes made to consent-based processing. Moreover, the aim of the research is to discuss the reason why consent is regarded as a lawful ground for the processing of personal data, in other words what the rationale behind having consent is. Through answering these questions this research tries to pursue the objective of describing consent under the upcoming GDPR, as well as elaborating on the origins of consent and its rationale in European data protection law. In short, the research *discusses the "now" and "then" of consent in European data protection law.*

1.3 Research questions

Because of the aforementioned research problem, I have formulated the following research question that this thesis will answer: 'How can the continued use of consent as a lawful ground for processing personal data in the GDPR be explained by the rationale behind consent and the changes made to consent under the former DPD framework?' This question in turn can be divided in the following research questions:

1. How are the legal grounds for processing personal data, in particular consent, regulated under the DPD framework?
2. What are the changes to the rules concerning consent (and their underlying reasons) made by the GDPR framework?
3. What is, from a regulatory perspective, the rationale for making consent one of the legal grounds of processing personal data?

1.4 Structure and approach

In general the methods that will be used during this research are doctrinal legal research and literature reviews. The first research question will be approached by analyzing the legal frameworks, as well as literature that can help in analyzing it. On top of this, relevant case law and Art. 29 Working Party documents on consent will be consulted. The focus of the first research question is describing the current legal framework concerning consent. For the

second research question the changes (and their motives) to the legal framework concerning consent are researched. For this research question documents from lawmakers will be researched. In addition to this, the legal framework will be analyzed. This research question is next to focusing on the changes themselves, focused on describing the 'why' behind the changes made to consent in the GPDR. For the third and last research question documents from the legislator and other important parties (such as the Art. 29 Working Party) will be researched, alongside legal literature on the subject concerning both national and international European data protection law. To answer this research question, consent and data protection law will not only be researched under the DPD and GDPR frameworks, but also before that. The focus with this research question is identifying the rationale behind consent in data protection law.

The structure of this thesis is as follows. After this first introductory chapter the next chapter (II) will explain the DPD data protection framework, in order to gain a good understanding of the present rules on processing personal data based on consent. In the third chapter (III) the changes (and their motives) to consent in the GDPR will be discussed, after which the fourth chapter (IV) will discuss the reasoning behind consent as a legal ground in EU data protection law. Hereafter the fifth and last chapter (V) will summarize what is concluded in the preceding chapters and give a final concluding answer to the research question which forms the basis of the thesis.

2. Consent as a lawful ground for processing personal data

Before proceeding to the next chapters that will delve deeper into the changes made to the DPD framework concerning consent-based processing and into the rationale behind consent as a lawful ground for processing, it is crucial to cover the DPD legal framework extensively and gain an understanding of the current law on consent-based processing. Consequently, this chapter will commence by describing the rules on lawful processing in general, after which the concept of consent will be introduced and the present legal framework on consent will be discussed. Hereafter will follow a conclusion to help answer the main research question of this thesis.

2.1 Rules on the lawfulness of processing personal data

Processing personal data cannot be done freely in Europe, as there is a right to privacy and a right to data protection in particular.[37] Processing personal data is furthermore only allowed when doing so according to certain principles. These important principles of European data protection law can be found in multiple sources and are almost identical.[38] They state (among other important things) that the act of processing personal data has to be lawful and fair, that the personal data is only collected for specified, explicit and legitimate purposes and that the collected data is adequate, relevant and not excessive in relation to the purpose for which they are processed. Besides this, the collected data has to be accurate, and it may not be kept for longer than is necessary for the purpose for which the data is collected.

Principles are however very general by nature, which leaves room for interpretation and discussion in concrete situations.[39] Because of this margin of interpretation the EU, for the sake of data protection in the internal market, deemed it necessary to have more detailed rules on EU level.[40] The EU therefore adopted more concrete rules in the DPD (and later the GDPR). Important rules that have been created are rules on the lawfulness of processing. These rules limit the number of grounds on which data may lawfully be processed, whilst also offering a basis to process personal data in a lawful way. This is important, as limitations of fundamental rights (like the right to privacy) in the ECHR need to be based on law.[41] This does however not seem mean that every data processing activity should automatically be seen

[37] Art. 8 ECHR and art. 8 EU Charter.
[38] Art. 6 DPD, art. 5 CoE convention 108 and art. 5 GDPR.
[39] Handbook on European data protection law, 2014, p. 80.
[40] Handbook on European data protection law, 2014, p. 80.
[41] Art. 8(2) ECHR.

as an interference under the ECHR, arguably because data processing activities differ enormously in both type and impact on privacy. Furthermore, personal data processing activities do not have to be harmful, but they do have a huge potential to be so. This opinion seems to be reinforced by CoE convention 108. In this convention the underlying idea is not that every data processing is an interference with privacy, but that to protect everyone's fundamental rights and freedoms, the processing of personal data should always fulfil certain conditions.[42] In addition, the OECD guidelines on privacy seem to share this idea of setting certain conditions to personal data processing. Nevertheless, under the EU data protection framework every data processing activity has to have a basis in law.[43] According to case law for a processing activity to be allowed it should comply with both the aforementioned principles and the rules on the lawfulness of processing.[44] The connection between the principles on the one hand and the rules on the other hand can be described as follows. The principles state that data must be processed lawfully, whilst the rules state that processing of personal data shall be lawful only and to the extent that at least one of the legal bases applies.[45] This connection is however not explicitly stated in both the DPD and GDPR. It would have therefore been wise, as De Hert and Papakonstantinou suggest, to clarify this connection in for example the recitals.[46]

2.1.1 The lawful grounds for processing personal data under the DPD

The rules on the lawfulness of processing under the DPD can be found in art. 7 and 8 of said directive. According to the directive, the availability of lawful grounds to base a processing activity on is depending on what type of personal data is to be processed. The directive differs between "regular" personal data and special (sensitive) categories of personal data. Sensitive personal data can be described as data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data that concerns health or sex life. [47]

[42] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', p. 6-7. See also Hustinx, *Statewatch 2013*, p. 6.
[43] See art. 8(2) EU Charter, art. 7 DPD and art. 6 GDPR.
[44] CJEU, Joined cases C-465/00, C-138/01 and C-139/01. Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk, 20 May 2003, para. 65 and CJEU, C-524/06, Huber v. Germany, 16 December 2008, para. 48.
[45] De Hert & Papakonstantinou, *Computer Law & Security Review* 2016, p. 186-187.
[46] See note 45.
[47] Art. 8 DPD.

When aiming to process regular personal data, there are a few legal grounds that could be utilized. A first ground is consent of the individual whose data will be processed, found in art. 7(a) DPD. This ground is, in brief, based on the permission of the individual to process the personal data. More about this legal ground will be discussed later during paragraph II.2. A second legal ground can be found in art. 7(b) DPD. This article states that processing is possible if the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract. This means a (pre)contractual relationship can also be a ground to base a processing activity on. A third legal ground stated in art. 7(c) DPD is possible if the processing is necessary for compliance with a legal obligation to which the controller is subject. A fourth possibility is art. 7(d) DPD, in case processing is necessary in order to protect the vital interests of the data subject. These interests are closely related to the survival of the data subject.[48] Moreover, art. 7(e) DPD states that, in case processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, processing is also possible. Finally, Art. 7(f) states a sixth and last ground to base the processing of personal data on. According to this article, processing is allowed if it is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed. This ground requires a balancing act, as the ground cannot be used when such interests are overridden by the interests for fundamental rights and freedoms of the subject should prevail. Apart from this balancing act, national law is not allowed to add conditions to the ones already mentioned in art. 7(f) DPD.[49]

When aiming to process sensitive personal data, the possibilities are different. Processing sensitive personal data is prohibited in art. 8(1) DPD, except in a few cases. Sensitive personal data may be processed if the data subject gives his explicit consent (about which more will be said later on), if the processing is necessary because of a legal obligation in the field of employment law, or if the processing is necessary to protect the vital interests of the data subject or another person where the subject is physically or legally incapable of giving his consent. Furthermore processing sensitive data is allowed in case it is carried out by a non-profit body with a political, philosophical, religious or trade-union aim and on condition that

[48] Handbook on European data protection law 2014, p. 83.
[49] CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011

the processing relates only to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data is not disclosed to third parties without the consent of the data subjects. Moreover, in case the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims, the processing is also lawful according to art. 8 DPD. Finally, according art. 8(4) DPD member states may create additional exceptions to the prohibition of art. 8(1) DPD for reasons of substantial public interest.

The relationship between the lawful grounds is not entirely clear. Consent is sometimes regarded as the most preferred ground, close to a constitutional principle, linked to the status of data protection as a fundamental right.[50] In the last chapter the contrary became visible: consent may in some cases actually provide individuals with a false sense of control and less data protection than expected. On the other side of the spectrum, art. 7(f) DPD "the legitimate interest" is sometimes seen as the least preferred ground, to be used as a left-over in cases where none of the other grounds would apply. [51] Art. 7(f) DPD should however not be regarded as the weakest link of the six grounds or an open door to legitimize all data processing activities.[52] Art. 7(f) has, opposed to the other grounds such as consent and performance of an agreement, a balancing test including additional safeguards such as the requirement to implement mitigating measures to minimize the impact on the privacy of individuals. It may therefore often provide better protection for individuals.[53] The DPD does furthermore not suggest any sign of hierarchy between the six different lawful grounds.[54] It should therefore be best to see the lawful grounds as six different grounds with no clear hierarchy and with different uses for different processing scenarios. The GDPR does not seem change this, as the regulation only states that processing shall be lawful if and to the extent at least one of the grounds applies.

2.1.2 The lawful grounds for processing personal data after the GDPR

Under the GDPR the same distinction is still made between regular personal data and sensitive personal data, depending on what type of information they reveal. New things that

[50] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 7.
[51] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', p. 9-10.
[52] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', p. 9-10.
[53] Moerel & Prins 2016, p. 48 – 49.
[54] Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', p. 9-10.

have been added are new categories of sensitive data such as genetic data, biometric data and information about sexual orientation. While extra protection for data about very private information is of course welcome, these rules still leave much room for improvement. It would be better to distinguish the data on the basis of the potential uses of data instead of on the basis of the nature of the information, because regular data can reveal sensitive data as well: one's name or meal could for example reveal his or her religion.[55] Regarding the lawful grounds for processing the GDPR brought some changes, whilst keeping all of the grounds. Notable changes are the prohibition of public authorities to use the legitimate interest as a lawful ground for the processing of regular personal data[56] and the addition of new grounds for processing sensitive personal data.[57] Furthermore concerning the processing of (sensitive) data on the basis of consent the GDPR brought many changes. These will be discussed during in chapter III. The changes to all the other grounds will however not be discussed extensively, as they are outside the scope of this research which focuses on consent in particular.

2.2 Consent as a lawful ground for processing personal data

Having introduced consent as one of the possible lawful grounds to base data processing activities on, this paragraph will delve into what the DPD states about consent as a lawful ground for processing personal data. The DPD is not very elaborate about consent – most of the information is originating from case law and from other parties such as the opinions originating from art. 29 Working Party. Information in the directive about consent can be found in the articles 2, 7, 8 and 26 of the DPD and in the recitals. In these articles the use of consent and its elements or building blocks are explained.

2.2.1 A valid consent according to the DPD

A valid consent under the DPD framework consists of a number of elements.[58] First there must any form of indication of wishes by which the data subject signifies his agreement. Secondly the action of consent must be freely given. Thirdly the given consent must be specific. Furthermore the consent must be informed. Lastly consent must be given unambiguously or explicit, depending on the nature of the personal data to be processed. These requirements will be now be discussed one by one.

[55] De Hert & Papakonstantinou, *Computer Law & Security Review* 2016, p. 183.
[56] Art. 6.1(f) GDPR.
[57] See art. 9.2(h) and art. 9.2(i) GDPR.
[58] Art. 2(h) DPD.

2.2.2 An indication of wishes by which the data subject signifies his agreement

The directive speaks of any indication of wishes in art. 2(h) DPD. It does not speak of any form in which this indication is to be given. There is in principle no limit as to the form consent can take.[59] What is necessary is an indication of wishes which is signified. This could be given in both oral and written form or reasonably derived from behavior, the last being for example dropping a business card in a glass bowl.[60] Another example of a situation in which consent can be derived from behavior is in case a person calls a specific telephone number in order to obtain local weather conditions. In this case by calling the number consent is constituted towards the service providing company to use the individual's location data.[61] Noteworthy however is the fact that unlike written consent, other types of consent will probably be considerably harder to prove they exist. Furthermore regarding the possible types of consent, it seems that there has to be a certain active behavior or action from where consent can be derived, and that passive consent, which is consenting through inaction, is not enough. This does however not mean that passive behavior can never lead to consent, as passive behavior accompanied by an action could be sufficient.[62] An example of this could be the silence of an individual combined with the fact that on an earlier point of time that individual had given a positive indication of his consent.[63] Other elements of consent and the requirement for consent to be unambiguous seem to support the interpretation that entirely passive consent is not possible.[64] Moreover, practice too supports this interpretation, as absence of active behavior of the data subject will pose problems for the data controller. The data controller in these cases will be unable to demonstrate that he has obtained lawful consent.[65] The DPD does not however explicitly preclude passive consent, ultimately leaving the question whether this in some cases will be possible and thus creating legal uncertainty.

Concerning the question when the act leading to consent has to be given the directive is silent too, although the language of the directive indicates that consent has to be given before the processing commences.[66] After all, "personal data may only be processed if … the data subject *has* unambiguously *given* his consent". Furthermore, consent under the DPD makes processing lawful. If consent would be obtained after the processing commences the

[59] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 11.
[60] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 11.
[61] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 12.
[62] Kosta 2013, p. 167.
[63] Kuner 2007, para 2.17.
[64] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 12.
[65] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 12.
[66] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 9.

processing carried out during the period without consent would be without a lawful basis, and if consent would be rejected during the processing the processing that would have taken place would also be unlawful. [67] Besides this, about the person giving the indication not much is stated by the DPD either. The directive does not go into the position of persons that are physical and/or legal incapable of giving their consent. The issues of physical or legal incapacity, including the conditions under which representation is allowed, are not regulated by the DPD but are instead left to the laws of member states.[68]

2.2.3 Freely given consent

Consent also has to be freely given according to the directive. What is to be understood as freely given consent is not explained by the DPD. According to the Working Party, this means that consent is only valid if the data subject is able to make a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent.[69] In other words, consent should be an autonomous act of the individual, free from external manipulations.[70] If this means that positive influencing, as opposed to negative influencing, makes a consent invalid is a difficult question. According to Kosta, applying positive pressure (such as offering personal benefits like discounts on products or services) does not invalidate consent to the extent that the individual has been provided with all the necessary information relating to the processing of his personal data and he has been given a real choice to decide.[71] If for example not consenting to having a supermarket costumer card results in only not receiving some price deductions on some goods, consent may still be valid. This is because the consequences are probably not serious enough to prevent a free choice.[72] However, the trouble with influencing acts like discounts is that it is hard to distinguish between positive and negative influence. Imagine a health insurance company selling insurances with discounts on the condition that additional personal data is shared with them. For some this might be a positive thing, however some that are in a financially tight situation might be practically forced to take the insurance which is discounted. Also imagine every health insurance company using this policy. The less fortunate individual will be faced with serious negative consequences if he or she does not consent, as he or she will not be insured.

---

[67] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 30-31.
[68] Kosta 2013, p. 160.
[69] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 12.
[70] Kosta 2013, p. 169.
[71] Kosta 2013, p. 172-173.
[72] Handbook on European data protection law, 2014, p. 58.

Regarding freely given consent the art. 29 Working Party has in some situations explored the limits of consent. According to the Working Party consent given under the threat of non-treatment or lower quality treatment in a medical situation is not considered as free.[73] Furthermore, where consent is not freely given if it is required from a worker if there is a real or potential relevant prejudice that arises from not consenting.[74] Moreover, regarding having 'a real choice' the Working Party questioned if consent could be used to transfer booking information of European airlines to U.S. authorities. The reason for this was that the airlines would be obliged to send this information before the flight departures, and that passengers because of this had no choice but to agree if they wanted to fly to the US.[75] The Working Party later stated that a free consent in this situation would not be possible.[76] Taking into account this statement by the Working Party, consent may be (or become) problematic for a lot of services. For example, as has been mentioned earlier, more and more of life happens 'on-line'. As many and perhaps most important social network sites use the consent of individuals to validate the processing of their personal data, one could argue that these individuals have no real choice as the practice is the same with every social network site.[77] This is problematic, because, especially for youth, much of their social lives happens online on these kind of websites. Denying consent, which in turn leads to denying them the access to these services, might have a big negative impact on their social lives and thus leaves them with no other option than to consent. Matzner et al also speak of similar problems. According to them, some IT services are actively advocated in education and the workplace by big IT companies, thereby spreading a lax data protection regime, which might be compulsory in school or at work.[78] In many cases these conditions can only be consented to, or evaded at high social costs, such as changing schools or employer.[79]

2.2.4 Specific consent

A very general consent is not a valid one, as consent must be specific. Extremely general consent, or so called blanket consent or open consent is also not acceptable.[80] This type of consent has no restrictions to its scope. Such consent may consist of agreeing to any use of

[73] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 13.
[74] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 13.
[75] Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC, p. 11.
[76] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 16.
[77] See social network sites such as www.facebook.com, www.twitter.com or www.linkedin.com for examples.
[78] Matzner et al 2016, p. 297.
[79] Matzner et al 2016, p. 297.
[80] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 17.

personal data and/or for any period of time. To be specific, consent must refer very precise to both the scope and the consequences of the data processing.[81] When the data controller undertakes different processing operations, consent does not always have to be renewed. It should be sufficient in principle for data controllers to obtain consent only once for different operations if they fall within the reasonable expectations of the data subject.[82] Furthermore in some situations if the data controller changes but the data processing remains the same renewed consent is also not necessary.[83] If the purpose of the data processing however changes, new consent may be needed according to the directive. Whether renewed consent is necessary is depending on the purpose(s) and the recipients of data.[84] Regarding the exact amount of specificity needed there seems no clear rule. Kosta states that the requirement has minimal literature about it, and that most literature about the requirement revolves around the specificity of information that should be provided to the individual which consent is needed.[85] This seems not very odd, as this requirement is closely tied to the next requirement that a consent should be informative.

2.2.5 Informed consent

This element of consent is closely related to the element of specific consent. The reason for this is that when data processing activities which have to be consented to are not specific and thus unclear, the data subject cannot be informed about these data processing activities.[86] The DPD does not say much about what constitutes an informed consent. According to the Working Party, informed consent means that the consent must be based upon an appreciation and understanding of the facts and implications of an action. This in turn means that the data subject must be given, in a clear and understandable manner, accurate and full information of all relevant issues, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject.[87] Additionally, the individual must be informed of the consequences of not consenting to the processing.[88] Moreover, the DPD states that information such as the identity of the controller and the

[81] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 17.
[82] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 17.
[83] See the ECJ C-543/09 Deutsche Telekom AG case at para. 65.
[84] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 18.
[85] Kosta 2013, p. 221.
[86] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 17.
[87] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 19. See also Article 29 Working Party, 'Working Document on the processing of personal data relating to health in electronic health records (EHR)', p. 9.
[88] Article 29 Working Party, 'Working document on the processing of personal data relating to health in electronic health records (EHR)', p. 9.

purpose of the processing should be given to the individual.[89] Informed consent is of special importance when transferring personal data to third countries, because of the possible lack of adequate protection in the concerned country.[90] On the basis of the aforementioned it could be argued that the more far-reaching the consequences are of the data processing in question the more the individual has to be informed. Yet not only informing individuals is important, it seems also crucial that the individual actually understands all the information he has received. The reason for this is that consent has to be given unambiguous, whilst someone with no understanding of what he is consenting to will likely not consent unambiguously. This idea is backed by the Working Party, which say that consent as in art. 2(h) DPD should be read together with further requirements mentioned later in the DPD, such as "unambiguous" and "explicit".[91]

Aside from the type of information to be given to the individual, there are two other important aspects to informed consent according to the Working Party. First the quality of the information must be sufficient. The way the information should be given (in plain text, without use of jargon, understandable etc.) depends on context.[92] If the average user for example is a child the information supply should be different than if the average user is an adult, as their language skills can differ greatly. Secondly the accessibility and visibility of the information to be provided is an issue. Information must be given directly to individuals, making it "available" somewhere else is not sufficient.[93]

Can an individual receive too much information? At first sight obtaining a lot of information might seem like a good idea, but according to Manson and O'Neill in the field of medicine making the rules concerning informed consent too strict have led to 'the development of increasingly complex, lengthy and (at worst) incomprehensible consent forms'.[94] The field of data protection seems also plagued by this problem, as exactly long and complex kinds of consent forms are probably one of the reasons individuals do not actively read or understand what they consent to.[95] To tackle this issue, O'Neill suggests giving individuals a limited amount of accurate and relevant information, providing them the opportunity to obtain more

[89] Art. 10 DPD.
[90] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 20.
[91] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 21.
[92] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 20.
[93] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 20.
[94] Manson & O'Neill 2007, p. 10 ff.
[95] Schermer et all speak of consent desensitization because of (among other things) an 'information overload', see Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16.

information in an easy way if they desire so, and allowing them to rescind consent once it has been given.[96] This task will however not be easy, as providing too few information will make consenting less meaningful as the individual is less informed, whilst providing too much information will perhaps result in individuals not reading the info at all, which is also detrimental to meaningful consent.

2.2.6 Consent in regular vs. sensitive personal data processing situations

Consent should finally be unambiguous or explicit. Which of the two is required depends on the nature of the data that is processed. Art. 7(a) DPD requires unambiguous consent for processing regular personal data, whilst art. 8.2(a) needs explicit consent for the consent to be valid when processing sensitive personal data. The directive sadly does however not state much about what exactly constitutes an unambiguous consent. According to the Working Party, unambiguous consent means that there is no doubt to the data subject's intention to deliver the consent.[97] This implicates that in case there is reasonable doubt to whether the consent is really meant or not, there is ambiguity and thus no unambiguous consent. This requirement forces data controllers to create multiple procedures for individuals to give their consent. On the one hand they must create procedures to obtain clear consent, and on the other hand they must create procedures to make sure that the person giving the consent is actually the data subject.[98]

Unambiguous consent can be given in multiple ways. One way to give unambiguous consent is by using written express statements, such as a signed agreement or written statements of the desire to agree.[99] It can also be given by express oral statements to signify agreement. [100] Sometimes unambiguous consent may even be inferred from certain actions, such as the example that was used earlier of throwing a business card in a bowl. This however is depending on whether the actions of the data subject lead to an unmistakable conclusion that consent in that case is given.[101] But should consent not always be unambiguous? According to Kosta the requirement does not add any real value to the interpretation of a valid consent because, according to her, the element 'unambiguously' is intrinsic in the concept of consent

[96] O'Neill, *Journal of Medical Ethics* 2003, p. 6.
[97] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 21.
[98] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 21.
[99] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 21.
[100] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 22.
[101] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 23.

and consent cannot be valid if it is ambiguous.[102] This approach to this element can also be found in certain member states implement the DPD, such as Sweden and Luxembourg.[103]

Explicit consent is essentially the same as express consent explained earlier.[104] Explicit consent can be given in both written form and orally. Although oral explicit consent is possible, oral is not advised as it is difficult to prove.[105] Inferred consent on the contrary will not normally be possible under art. 8(2) DPD. The reason for this is most likely that inferred consent (implicit consent) is based on behavior, which is harder to interpret and requires more context.

2.2.7 Consent as a requirement in case of certain data transfers

Data can be transferred from one country to another country, while both countries can have different rules concerning data processing. Between EU member states this should be no problem, as the DPD and its implementations are in force which guard a certain level of data protecting. When pursuing a personal data transfer to third countries outside of the EU however this is not the case, and the transfer is only allowed when the third country ensures an adequate level of (data) protection.[106] There are however exceptions to this rule, one of them involving unambiguous consent. According to the DPD, the unambiguous consent of an individual may legitimize a personal data transfer to a third country that does not provide for an adequate level of data protection.[107]

2.2.8 Consent in the DPD and lack of a harmonized interpretation

As the DPD is a directive it has to be implemented in national member state law. In implementing the directive, many member states seem to have interpreted different aspects of consent differently. This lack of a harmonized approach between member states is recognized by the EU. The Commission states that consent conditions sometimes vary greatly, ranging from a general requirement of written consent to the acceptance of implicit consent.[108] This lack of a harmonized approach can also be observed by the fact that most member states have

[102] Kosta 2013, p. 235.
[103] Kosta 2013, p. 235. See also Korff, *Londen Metropolitan University* 2010, p.70.
[104] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 25.
[105] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 25.
[106] Art. 25(1) DPD.
[107] Art. 26(1)(a) DPD.
[108] COM (2010) 609 final, p. 8.

defined consent in their laws, whilst some member states such as the UK and France have not.[109]

2.3 Interim conclusion

Processing personal data is only allowed when doing so in according with important data protection principles. Because of the general nature of principles however, certain rules are also created. One important type of rules that is created concern the lawfulness of processing. These rules on the lawfulness of processing limit the number of grounds on which personal data may be processed on the one hand, whilst also offering a basis for personal data processing on the other hand. According to these rules personal data may be processed on a number of grounds. These have no real hierarchy between and should be seen as providing uses in different processing scenarios.

Consent forms one of these important grounds for lawful processing. Following the directive, a valid consent should be freely given, specific, informed and unambiguous or explicit, depending on whether regular or sensitive data is to be processed. Apart from stating the requirements of a valid consent, the directive is rather silent on consent. More clarity on consent has to be obtained from other sources, such as documents from the Working Party and literature on consent. The analysis of the current law thus shows that there is room for improvement. Not only does the DPD state little about consent in particular, its understanding and implementation is also fragmented in the member states of the EU. Clarifying consent in a new regulation will therefore probably not only offer more protection to individuals, by for example more clearly stating how an individual should be informed, but will also tackle the harmonization problem which improves the data protection of individuals as well.

[109] Kosta 2013, p. 149 – 150.

3. The GDPR and its changes to consent

In order to be able to answer the question how the continued use of consent can be explained by the changes to the rules concerning consent that came with the GDPR reform and by the rationale of consent, it is essential to describe the changes that the GDPR has brought along with their motives. As a result of this, this chapter will start off by shortly discussing the reason why the DPD framework was departed in favor of the GDPR. Hereafter the changes to consent (and their motives) will be discussed one by one, after which a concluding paragraph will follow summarizing all findings.

3.1 The GDPR, its objectives and the reason for change

The GDPR brings quite a few new things compared to the DPD regarding both consent and other important data protection aspects.[110] According to the Commission the primary objectives of the GDPR however stay the same as the objectives of the DPD: to protect the fundamental rights and freedoms of individuals, in particular the right to data protection, on the one hand and promoting the free flow of personal data, thereby achieving an internal market, on the other hand.[111] The changes to the data protection framework, including those to consent, should therefore first and foremost be seen as an attempt to strengthen the pursuit of these aforementioned goals. Another reason for change can be found in the fact that the DPD has not prevented fragmentation, legal uncertainty and a widespread public perception that online activities are risky.[112]As a result of this, a "*stronger and more coherent data protection framework, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities*" was deemed necessary by the Commission.[113] The GDPR could furthermore be seen as a consequence of the Commissions wish to modernize the EU data protection framework, allowing it to continue to be a driving force in promoting a high level of data protection on a worldwide scale.[114]

3.2 The changes to consent

The changes regarding consent as a lawful ground for processing personal data will now be discussed. Apart from introducing some new things to consent, current rules concerning

[110] See paragraph 1.1 of this thesis for examples.
[111] COM (2010) 609 final, p. 2.
[112] COM (2012) 11 final, p. 2.
[113] COM (2012) 11 final, p. 2. See also rec. 7 of the GDPR.
[114] COM (2010) 609 final, p. 5.

consent are also made clearer through the articles and recitals of the GDPR. The GDPR has brought some changes to the requirements of a valid consent, introduced a right to withdraw consent, introduced a burden of proof for data controllers to prove an individual has consented and formulated special rules concerning consent by minors. Noteworthy is the fact that making consent stricter, by using a narrow interpretation of the concept and adding more formal requirements, does not per se improve the data protection of individuals. According to Purtova, consent, which is one of the most important control rights, loses significance as a ground of lawful processing when the strengthened formal requirements to consent are difficult to comply with.[115] Moreover, Schermer et al. argue in this context that consent will lose its value in practice when consent is made stricter in the sense that it is always required to be explicit (a proposed change that has (luckily) not made it into the final text of the GDPR).[116] It therefore remains a question if the changes to consent actually will improve the data protection of individuals.

3.2.1 The act of consenting under the GDPR

Many of the changes that the GDPR bring concern the requirements of a valid consent. The GDPR does not abandon old or create new requirements, but instead clarifies already known concepts. A first difference in the regulation compared to the old directive is that the regulation specifically states that "consent has to be given by a statement or affirmative action."[117] Furthermore, the same recital states that "silence, pre-ticked boxes, inactivity, failure to opt-out or passive acquiescence do not constitute valid consent". As a result of this, passive or 'opt-out' consent is therefore officially declared impossible, and only opt-in consent (consent by affirmative action[118]) is allowed. Additionally, by answering the question whether passive consent is allowed negatively the GDPR has improved the legal certainty surrounding consent. This change does however not seem to mean that implicit consent is ruled out by the GDPR. According to the regulation consent can be given by any "statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing".[119] The reason for this change can most likely be found in the general wish to clarify and possibly harmonize all the EU member state laws regarding consent and other data protection aspects, benefitting the EU internal market and offering a uniform level

[115] Purtova, Computer Law and Security Review 2013, no. 016/2013, p. 21.
[116] Schermer, Custers & Van der Hof, Ethics Inf Technol 2014/16, p. 172.
[117] Rec. 32 GDPR.
[118] Kuner 2007, para 2.17.
[119] Rec. 32 GPDR.

of data protection. This is because the working party already had a similar view concerning passive consent[120]. Additionally, full silence in order to deliver a valid consent has been regarded as impossible in literature as well.[121]

3.2.2 Freely given consent under the GDPR

A second difference concerns the fact that consent must be given freely. According to the GPDR consent should not provide a valid legal ground for the processing of personal data in case there is a clear imbalance between the data subject and the controller, especially when the data controller is a public authority.[122] This may implicate that consent should no longer be regarded as a good legal ground for certain processing activities between public authorities and citizens or employers and employees, as in those contexts there is an inherent imbalance between the two parties. The original proposal for the GDPR made by the Commission included the employee vs employer relationship in its initial text, however it seems to have vanished in the definitive version.[123] Nonetheless, consent in employment contexts is generally regarded as inappropriate. According to the Working Party it is misleading if an employer seeks to legitimize the processing of the data of his employee through consent. [124] In some employment contexts however consent might have its uses, provided there are guarantees that consent is really free.[125] But also outside of these situations of public authority vs citizen or employer vs employee consent might not be a good basis for data processing, as the regulation speaks of a clear imbalance between a data subject and a data controller in general. Whether this addition is good or not is debatable. According to Purtova consent loses importance because of this change.[126] It seems that because of this somewhat paternalistic measure all individuals will lose some of their freedom to use consent, in order to better protect some individuals.

Another addition that the regulation brings can be found in recital 43 of the regulation: consent is presumed to be not freely given if it does not allow separate consent to be given to different personal data processing operations, despite it being appropriate in the individual case, or if the performance of a contract is dependent on the consent despite such consent is

[120] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 12.
[121] See Kosta 2013, p. 167 & Kuner 2007, para 2.17.
[122] Rec. 43 GDPR.
[123] Compare rec. 34 of the draft data protection regulation with rec. 43 of the definitive version of the GDPR.
[124] Article 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context, p. 3.
[125] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 14.
[126] Purtova, Computer Law and Security Review 2013, no. 016/20013, p. 14.

not necessary for such performance.[127] Especially this last sentence requires some attention. According to the regulation when the performance of a contract, including the provision of a service, does not require the processing of the individuals data but it nonetheless is asked for the consent is presumed to not have been given freely. This is emphasized upon not only in the recitals but also in the articles of the regulation itself.[128] Consent should thus not be bundled with other contracts. Finally, consent according to the regulation should not be regarded as freely given in case the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[129] This last sentence contains the essence of a freely given consent and is probably formulated to clarify what constitutes a free consent. The part that consent should be able to be withdrawn without detriment is new, possibly preventing "punishments" to individuals that want to withdraw their consent.

The motive behind these changes can most likely be found in the wish to harmonize the conditions of a valid consent. The Commission noted in their (compulsory) impact assessment that the requirement of "free consent" needed clarification. According to the Commission the Working Party has given guiding opinions on this matter, but this has not solved the problem of divergent national approaches.[130] By harmonizing these rules about consent, a uniform (high) level of data protection within the EU is ensured and the internal market of the EU is safeguarded.

3.2.3 Informed consent under the GDPR

Informed consent received more clarity too under the GDPR. According to the regulation, a pre-formulated consent declaration should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.[131] For guidance on what exactly can be seen as clear language or an unfair term, the directive 93/13EEC can be consulted.[132] This directive seems to have been the source of inspiration for this obligation. Moreover, according to the Commission transparency is key in providing individuals with control over their data and ensuring effective protection of personal data.[133] Most likely as a

[127] Rec. 43 GDPR.
[128] Art. 7(4) GDPR.
[129] Rec. 42 GPDR.
[130] European Commission, Evaluation of the implementation of the data protection directive p. 19.
[131] Rec. 42 GDPR.
[132] Directive 93/13/EEC on unfair terms in consumer contracts.
[133] COM (2010) 609 final, p. 6.

result of this, transparency can also be found as a new principle in the GDPR.[134] This principle requires that any information or communication relating to the data processing of individuals has to be easily accessible and easy to understand.[135]. As a result, the principle creates a data processing environment of trust.[136] This trust is important according to the Commission for the development of a digital economy in the internal market.[137]The regulation furthermore states that the data subject must also be made aware of at least the identity of the data controller and the purposes for which the personal data are intended.[138] According to the regulation, these topics should at least be addressed for a consent to be informed. This does however serve as a minimum, and more information might be necessary in certain situations. According to the regulation "*natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing."*[139] This however seems part of a general obligation to inform individuals, not necessarily a requirement for creating an informed consent. The regulation also mentions that "*if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided".* [140] In the online reality information is usually given to the individual by privacy policies and notices, to which the individual has to consent to.[141] These policies and notices are however not always clear, making it often difficult for individuals to understand and to give their informed consent.[142] This change can probably be seen as an attempt to address these practices. Furthermore, this sentence causes one to rethink current cookie law, which adds huge pop-ups blocking entire webpages, thereby being unnecessarily disruptive. These additions to informed consent in the regulation seems to address both the requirement of quality of information and accessibility and visibility of information mentioned by the Working Party.[143] This is important because individuals have to be well-informed in order to make good decisions about their personal data.

3.2.4 A right to withdraw consent

[134] Art. 5(1)(a) GDPR.
[135] Rec. 39 GDPR.
[136] De Hert & Papakonstantinou, *Computer Law & Security Review* 2016, p. 134.
[137] Rec. 7 GDPR.
[138] Rec. 42 GDPR.
[139] Rec. 39 GDPR, see also art. 7(3) GDPR.
[140] Rec. 32 GDPR.
[141] Kosta 2013, p. 215.
[142] COM (2010) 609 final, p. 9. See also the earlier mentioned Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16
[143] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 20. See para 2.2.5 of this thesis.

According to the regulation the data subject shall have the right to withdraw his or her consent at any time and the withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal. [144] This means that the withdrawal of consent is only effective for future data processing after the withdrawal. This is an important difference with the right to be forgotten (also right to erasure) that is also added to the data protection framework by the GDPR.[145] This right allows past information to be erased after invoking it. The idea of a possibility to withdraw consent is not new, as it is implicit in the DPD.[146] National implementations of the DPD furthermore also mentioned the withdrawal of consent as an option, such as the Greek Data Protection Law.[147] Thus can be said that this change is more of an affirmation of already existing (implied) rules. The reason for this change therefore seems primarily to be based on harmonization, trying to level the data protection within the EU.

The regulation does seem to add something new though. A novelty that can be observed is the obligation that the withdrawal of consent must be as easy as giving consent. This may implicate that the withdrawal of consent may be mere clicks away. From the perspective of the individual, this rule seems to add much to his personal data protection. It offers him more control over the processing of his personal data, allowing him to stop the processing of his data if he desires so later on. This can be valuable when, after providing consent, the data processing or its effects prove to be undesirable. From the perspective of the data controller this addition to the right to withdraw consent is likely to make consent a less preferred ground to base the processing of personal data on. The reason for this is that consent can become an unsafe option, as consent could be withdrawn at any time and for any reason.

3.2.5 Demonstrating consent

Another change can be found in art. 7(1) GDPR. According to this article the controller is required to be able to demonstrate that the data subject has consented to the processing of his or her personal data. This change can be linked to the accountability principle, a new principle found in the GDPR.[148] According to this principle merely abiding the data protection rules is not enough, showing compliance with the rules is also mandatory. The accountability

[144] Art. 7(3) GDPR.
[145] Art. 17 GDPR. See also ECJ C-131/12 Google Spain v. AEPD where the right to be forgotten was introduced.
[146] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 32.
[147] Kosta 2013, p. 215
[148] New as meaning novel in the EU framework of DPD and GDPR. The Working Party states that the concept is not new, as it is recognized in for example the OECD privacy guidelines and the APEC privacy framework. See also Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability', p. 6.

principle requires data controllers to implement measures to effectuate the data protection principles and obligations and to demonstrate their compliance on request.[149] Back to the obligation to demonstrate consent this means that under the GDPR gathering evidence of given consent is crucial, as this is necessary to be able to demonstrate consent later on if needed. This situation differs from the DPD, as under the directive gathering evidence was not obligatory, although recommended for cases when consent has to be proven, such as possible disputes.[150]

3.2.6 Consent and minors

A last change to the regulation concerns consent in the case of minors. According to the Commission children deserve extra protection. They deserve this protection as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[151] Rules about other groups of individuals that are incapable of giving a valid consent do not seem to have been addressed in the regulation, even though it has been requested by some.[152] The extra protection for minors can be found in art. 8 of the GDPR. The regulation requires a child's consent in relation to information society services to be authorized by their legal representatives (which in most cases would be the parents).[153] According to the regulation, this authorization is required until the child is at least 16 years old. Moreover, member state law may provide for an even lower age requirement, as long as it does not go below 13 years. The regulation states one exception to obligatory authorization: it is not required in case of preventive or counselling services offered directly to a child. To determine whether an authorization is necessary, the meaning of an information society service can be found between the definitions found in the regulation. An 'information society service' means a service as defined in art. 1(1)(b) of Directive 2015/1535.[154] Following this directive, the definition of information society services is "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".[155] This implicates that pretty much every online commercial service is affected,

[149] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability', p. 3.
[150] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent', p. 21.
[151] Rec. 38 GDPR. See also the Internet for Children qualitative study, available at http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf. This study shows that children underestimate risks and deny or minimize the consequences of the internet.
[152] European Data Protection Supervisor, 'Opinion on the data protection reform package (2012), p. 22, Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals, p. 13.
[153] Art. 8(1) GDPR.
[154] Art. 4(25) GDPR.
[155] Art. 1(1)(b) Directive 2015/1535.

such as the ever-popular social network sites. In order determine whether authorization is required in a certain case, data controllers are obligated to make reasonable effort in verifying whether the consent of a child is authorized by the legal representative, taking into consideration available technology.[156] This rule seems very dynamic and able to withstand technological progress, thereby ensuring that age verification remains sound.

3.2.7 Impact of the GDPR on already given consent

Consent is an important way of legitimizing personal data processing, both under the DPD and the GDPR. This raises the question what the changes to consent mean for already existing consent. Luckily the GDPR offers an answer to this question. According to the regulation DPD-consents will remain valid, granted they are already in line with the conditions of the regulation.[157] This means that when a consent is GPDR-proof a data controller can continue with his data processing operations, and no extra actions are required. However, due to some of the changes a lot of individuals might need to be asked for their renewed consent.

3.3 Interim conclusion

Both the DPD and the GDPR have two main goals that have not changed: ensuring a high level of data protection and achieving a internal market within the EU. The changes to the framework, such as those to consent should therefore generally be seen as an attempt to strengthen to pursuit of these goals. Due to the wording of the GDPR and the addition of individual rights and stricter regulation, it can be argued that the GDPR primarily attempts to improve the data protection of individuals. Concerning the requirements for a valid consent the regulatory framework has received quite a few changes. A major change is that passive consent is ruled out in the regulation, by stating that an affirmative action is required and silence, pre-ticked boxes, inactivity etc. do not constitute valid consent. Another change is that the GDPR now states that consent should not be used in situations where there is a clear imbalance between the data controller and the individual, such as in government vs. citizen and employer vs. employee relations. Moreover, the GDPR presumes consent to not have been freely given if the use of consent for one data processing operation is compulsory bundled with different data processing operations or if consent is used for the performance of a contract, whilst the consent is not actually necessary for that performance. In addition to these changes, informed consent has so received clarity. According to the changes pre-

[156] Art. 8(2) GDPR.
[157] Rec. 71 GDPR.

formulated consent declarations should be provided in an easily accessible form, with clear and plain language. Additionally, if consent is asked online the request must be clear and not unnecessarily disruptive to the use of the service for which the consent is asked. This means unreasonably long and unclear privacy policies should be a thing of the past.

Next to the requirements for a valid consent, the GDPR also brings changes regarding other topics relating to consent. A first change is the introduction of the right to withdraw consent. Primarily the addition of the rule that withdrawing consent should be as easy as it is given is novel. A second change is that the withdrawal of consent should be without detriment, thereby prohibiting "punishments" for withdrawing consent. A third change is that data controllers are obligated to demonstrate the existence of consent if asked. This means gathering evidence of a given consent has become crucial. A third change concerns consent given by minors. When providing information society services to children aged under 16 (parental) authorization is required. In addition to this, data controllers have to take measures to verify the age of individuals in order to determine whether authorization is required.

To conclude the discussed changes made to consent seem to sometimes add new concepts, such as the rules about parental authorization and the rules concerning the obligation to demonstrate consent, but in many case clarify known concepts. As a result of these changes consent as a lawful ground for processing personal data has become more harmonized in the EU, offering the same level of data protection to all member states. Certain concepts are furthermore made clearer, such as what constitutes an informed consent. Many of these topics were addressed before by the Working Party and others, but these are still important changes as the documents of these groups are not legally binding. Finally, these changes show that consent remains important, although becoming increasingly difficult to properly use due to its stricter requirements. It would seem that these stricter requirements improve the data protection of individuals instead of weakening their position. These changes to consent's elements "informed" and "freely given" will make consent more meaningful, whilst the rules concerning withdrawing consent offer individuals more control. In addition, the extra rules concerning minors offer them more protection. There is also a drawback to stricter requirements as it might make consent less used, limiting the control of individuals. This concerns the rules of consent not being viable in case of clear imbalance between the individual and data controller. This drawback however seems to not outweigh the benefits of these changes.

4. The rationale behind consent

In this fourth chapter the rationale behind consent will be discussed, to explain why consent is regarded as an important way of legitimizing data processing operations. This chapter starts off by discussing the increasing importance of the rationale behind consent in national European data protection law. Afterwards, the rationale of consent relating to the OECD Guidelines concerning privacy, CoE convention 108, DPD and GDPR will be discussed. Finally, this chapter will end with a conclusion.

4.1 The birth of informational self-determination in (parts of) Europe

The rationale behind consent is closely tied to the focus and rationale of data protection laws in general. Data protection laws have been adopted by most European nations since 1970.[158] Both technology and data protection have however not stood still since then, as the focus of data protection has not remained the same as in 1970. This switch in focus will now be discussed, from the focus on what Mayer-Schönberger calls the 'taming of technology' during the early years of European data protection law, to the increased emphasize on individual privacy in later data protection documents and ultimately the GDPR and its strengthening of the individuals' right to control his or her personal data.

4.1.1 Early data protection legislation

The first European data protection laws were enacted in the 1970s. The first data protection law created in the world is the Hessian Data Protection Act, which was adopted in 1970.[159] The first national data protection law came however not from Germany but from Sweden instead. In 1973 Sweden enacted the world's first national data protection law, named the Swedish Data Act.[160] According to Mayer-Schönberger these first generation data protection laws, along with the data protection statute of the German state if Rheinland-Pfalz, the proposals for a German Federal Data protection Act and Austrian proposals for a Data Protection Act, were all enacted for the same reason. According to him, they are direct reactions to planned centralized national data banks.[161] The demand for these data banks can be explained by two developments that came about around the same time: computerization and upcoming government bureaucracy.[162]

[158] V. Mayer-Schönberger 1997, p. 219.
[159] Kosta 2013, p. 45.
[160] Kosta 2013, p. 35.
[161] Mayer-Schönberger 1997, p. 221.
[162] Mayer-Schönberger 1997, p. 222.

In the case of Sweden for example, their early legislative act (being the first national act in the world) can be explained by the fact that computerization happened early. The reason for this is that the relatively small population combined with a high standard of living favored the development of ICT in Sweden.[163] Moreover, Sweden was a good place to start with automated registers, as public authorities already kept many records with information of the Swedish citizens.[164]

The creation of these registers or databanks did however not happen without public resistance. Citizens feared an automated and dehumanized bureaucracy, with technology being the problem.[165] In Sweden for example the privacy debate ignited after the (computerized) Swedish population and housing census of 1970, which was surprising as similar consensuses had taken place earlier in 1960 and 1965.[166] The computer seemed to be the problem, and the use of computers had to be regulated and controlled.[167] As a result of this, most of the first-generation norms can be seen as an answer to these problems. They do not focus on the direct protection of individual privacy (if understood as control) but they focus on the function of data processing in society.[168] According to Mayer-Schönberger data protection norms during this time were seen as a part of an attempt to tame technology: the use of data processing had to be regulated to ensure it was in line with the goals of society.[169] As a consequence, most of these data protection rules were not aimed at the individuals to ensure their compliance, but instead at special institutions which had to supervise compliance of the data controllers to these rules.[170]

The instigators of the first data protection laws, the centralized databanks, were however not fully realized in the end. Part of this can be attributed to the opposition by citizens, but another reason for this is because technology developed in another direction. [171] So called minicomputers came about and this allowed smaller government-related or business-related organizations to apply electronic data processing.[172] The reason for this can be found in the

[163] Kosta 2013, p. 36.
[164] Kosta 2013, p. 36.
[165] Mayer-Schönberger 1997, p. 223.
[166] Ilshammar, *Human IT* 2007, no. 9/1, p.13.
[167] Mayer-Schönberger 1997, p. 223.
[168] Mayer-Schönberger 1997, p. 223.
[169] Mayer-Schönberger 1997, p. 223.
[170] Mayer-Schönberger 1997, p. 224.
[171] Mayer-Schönberger 1997, p. 225.
[172] Mayer-Schönberger 1997, p. 225.

fact that minicomputers were smaller, less powerful but in turn also less expensive than mainframe computers; in fact they were designed to appeal to small and medium sized organizations.[173] The original relatively small amount of possible data protection violators grew exponentially into a huge amount of potential violators as a result of this, leading to a shift in the data protection discussion.[174] An increasing amount of European citizens wanted not only legislation aimed at attempting to control data processing technology, but also individual privacy and data protection rights.[175]

4.1.2 Increased emphasize on individual privacy

The aforementioned wish ultimately led to a second generation of data protection norms according to Mayer-Schönberger. From now on data protection was linked to the right of privacy, and consequently data protection was seen as the right of the individual to ward off society in personal matters.[176] The second generation rules seem similar to the first generation rules, but they are a few differences. Technical jargon has been removed, definitions have become abstract (technology-neutral) and existing individual rights were improved.[177] According to Mayer-Schönberg the French, Austrian, Danish and Norwegian data protection statutes can be seen as the beginning of this second generation of data protection legislation.[178] Moreover, during the first generation of rules individuals had the right to access and correct his or her personal data but these were interpreted functionally, in other words, they were installed to improve the accuracy of the data that was processed.[179] Individuals could thus do something about the data, but not stop data processing entirely. However with the coming of the second generation this changed, and individuals actually started to have say in the data processing process.[180] Consent sometimes became a precondition for personal data processing, individuals could in some cases permit data processing that otherwise would be prohibited and more: for example in the Norwegian Data Act there was laid down that individuals could refuse data processing for direct marketing or market research.[181] The thought that individuals would be best suited to protect their personal data became leading.[182]

[173] Estabrooks 1995, p. 53.
[174] Mayer-Schönberger 1997, p. 225.
[175] Mayer-Schönberger 1997, p. 225.
[176] Mayer-Schönberger 1997, p. 226.
[177] Mayer-Schönberger 1997, p. 226.
[178] Mayer-Schönberger 1997, p. 226.
[179] Mayer-Schönberger 1997, p. 226.
[180] Mayer-Schönberger 1997, p. 227.
[181] Mayer-Schönberger 1997, p. 227.
[182] Mayer-Schönberger 1997, p. 227.

Moreover, during this generation, data protection was no longer seen as an attempt to regulate technology but it became an individual freedom of citizens.[183] This change, however, did not really work. Citizens and society are so connected that resisting information requests is either impossible or possible but at a great social cost.[184] Consequently, in real life the individual did not really have the opportunity to decide whether he took part or remained outside society. The question to whether this course of events was the way to go eventually led to a new generation of data protection norms.

4.1.3 The right to informational self-determination

And so came an end to the second generation, after which came a new generation. This third generation changed data protection from an individual liberty to ward off (informational) privacy invasions to a participatory right to informational self-determination.[185] Instead of the question whether an individual wanted to take part in societal processes the question *how* the individual wanted to take part became important.[186] This view corresponds to Westins idea of privacy. According to him, "*privacy is the claim of individuals, groups and institutions to determine for themselves when, how, and to what extent information about them is communicated to others*".[187] New technological developments and their legal challenges affected data protection law during the second and third generation; because of these the lawmakers retreated from active regulation of technology. Instead of persisting along a difficult path of continuous adaptation of technology-shaping legislation, politicians had chosen to concentrate on more individual liberties and participation rights.[188] Consequently, the third generation of data protection norms emphasized participation and self-determination.[189]

Information self-determination in the beginning was made popular by the German Constitutional Court (the Bundesverfassungsgericht) in 1983 with its population census decision.[190] This case was about a German attempt to conduct a population census in 1983. The act that made the population census possible did not receive much resistance, however in

[183] Mayer-Schönberger 1997, p. 227.
[184] Mayer-Schönberger 1997, p. 228.
[185] Mayer-Schönberger 1997, p. 229.
[186] Mayer-Schönberger 1997, p. 229.
[187] Westin 1970, p. 7.
[188] Mayer-Schönberger 1997, p. 230.
[189] Mayer-Schönberger 1997, p. 231.
[190] BverfGE 65,1 of 15 december 1983 (Volkszählung)

strong contrast with this the societal debate around it was huge.[191] Moreover, besides a very heated debate the act was also brought before German courts, ultimately coming before the German Constitutional Court. The decision of this court ultimately upheld the aim of the population census, but demanded further procedural and organizational safeguards to protect the fundamental rights of citizens.[192] The population census was however not stopped but postponed, as a new act that would allow the population census was passed later on, deemed constitutional by the constitutional court and conducted in 1987.[193] Nonetheless the judgement of the court has been very important. In its judgement, the court stated that the right of information self-determination was a constitutional fundamental right.[194] Moreover, it was an implementation of a general right of personality, which was made up of on the one hand the protection of dignity and on the other hand the protection of general personal liberty.[195] Furthermore, the right guaranteed the ability of the individual to decide or determine the release and use of his personal data (hence the name information self-determination).[196] The right to information self-determination is not absolute, though, and other interests have to be balanced with this right.[197] Important parts of the reasoning of the court are based on ideas from the sociological systems theory, in particular the works of Niklas Luhmann.[198]

According to Kosta, the right to information self-determination as set out in the population census case greatly influenced greatly data protection legislation in many European member states, placing the individual in a position to determine how he would participate in society.[199] Bygrave, more nuancedly, notes that it had a considerable impact on development of data privacy law and policy in Germany, and, to a lesser extent in other European countries.[200] What could be said however is that because of the right of information self-determination the concept of consent gained importance.[201] The reason for this can be found in the fact that consent is an, if not the most, important way of controlling your own personal data. Withholding consent may mean data processing will not be able to take place (if none of the

[191] Hornung & Schnabel, *Computer Law and Security Review 2009/25,* p. 85.
[192] Hornung & Schnabel, *Computer Law and Security Review 2009/25,* p. 85.
[193] Hornung & Schnabel, *Computer Law and Security Review 2009/25,* p. 85.
[194] Hornung & Schnabel, *Computer Law and Security Review 2009/25,* p. 86.
[195] Hornung & Schnabel, *Computer Law and Security Review 2009/25*, p. 86.
[196] Mayer-Schönberger 1997, p. 229.
[197] Rouvroy and Poullet 2009, p. 56.
[198] Hornung & Schnabel, *Computer Law and Security Review 2009/25*, p. 85. See also Luhmann 1965.
[199] Kosta 2013, p. 52.
[200] Bygrave 2004, p. 323.
[201] Kosta 2013, p. 52.

other legal grounds can be utilized), whilst giving consent will mean the exact opposite. According to Roßnagel et al consent can be seen as the "genuine expression of the right to informational self-determination".[202] It could however be argued that most of the real shift towards information self-determination happened in Germany, which is logical as it was created there. According to González Fuster, consent was one of the major peculiarities of the BDSG, the German national law.[203] Kosta mentions that countries like Austria, Norway and Finland amended their legislation to integrate the right to informational self-determination.[204]

Emphasizing on participation and control however turned out not to have the desired effects. Even with improved participatory rights, individuals were not willing to pay the monetary and social cost of exercising their right of informational self-determination.[205] Furthermore, individuals also (routinely and unknowingly) contracted away their right to informational self-determination.[206] According to Mayer-Schönberger data protection mostly remained a privilege of minorities of those who could afford to exercise their rights.[207] As a result of the weak position of individuals came the fourth generation of data protection norms. This fourth generation can be characterized by new sectoral legislation and norms trying to strengthen the individual's position against information gathering institutions and trying to stop the bargaining of data protection-related rights.[208] Examples of these norms are the introduction of no-fault compensation for data protection claims, the prohibition of processing sensitive data (thereby stopping the bargaining of the right to process these data) and the addition of new enforcement institutions.[209] With the fourth generation data protection norms the right to information self-determination kept the same role as before, yet it is now enforced, detailed, supplemented and supported, thereby improving the concept.[210] According to Mayer-Schönberger the DPD follows this evolution. In the directive individual participation rights are important, consent has a prominent role within the data processing scene, individuals in some cases have the right to object data processing and effective enforcement is ensured.[211]

[202] Kosta 2013, p. 109. See also Roßnagel, *Bundesministerium des Innern, p. 15*.
[203] González Fuster 2014, p. 60.
[204] Kosta 2013, p. 106.
[205] Mayer-Schönberger 1997, 232.
[206] Mayer-Schönberger 1997, 232.
[207] Mayer-Schönberger 1997, 232.
[208] Mayer-Schönberger 1997, 232 – 233.
[209] Mayer-Schönberger 1997, 233.
[210] Mayer-Schönberger 1997, 234.
[211] Mayer-Schönberger 1997, 234 – 235.

4.2 Information self-determination and international data protection frameworks

As we have seen, the concept of information self-determination has been prevalent in some national data protection laws for quite some time. In this paragraph the influence of information self-determination shall be discussed under the CoE convention 108, OECD guidelines, and under the DPD and GDPR frameworks.

4.2.1 Informational self-determination, the OECD Guidelines and CoE convention 108

Information self-determination does not appear to play a big role in both CoE convention 108 and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These OECD Guidelines provide basic rules that govern the protection of personal data and privacy, however its scope is limited to personal data '*which because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties*', implying a threshold condition for protection of personal data.[212] This seems to be not in line with the idea of informational self-determination, which is that one should be able to decide or determine the release and use of his personal data.

Furthermore not many traces of consent, a key notion according to informational self-determination, can be found in the OECD guidelines. The OECD Guidelines only mention consent in two occasions. The OECD Guidelines state under the collection limitation principle that '*there should be limits to the collection of personal data, and that such data should be obtained by lawful and fair means and, where appropriate, with the knowledge of consent of the data subject'*. The guidelines do however not make it clear when consent is or isn't required.[213] Enlightening a bit when consent is required, the OECD Guidelines state that Personal Data 's*hould not be used for purposes other than those specified in accordance with the purpose specification principle except when the consent of the data subject is obtained, or by authority of law'*.[214] The OECD Guidelines offer no other clarification as to what exactly constitutes a consent, and if and when consent is required in other situations. The OECD Guidelines do have an individual participation principle, but this principle is aimed at providing individuals with information about data processing operations and allowing them to challenge (incorrect) data about them, not granting them control over when and how their data

[212] Hustinx, *Statewatch 2013*, p. 8.
[213] Kosta 2013, p. 32.
[214] Kosta 2013, p. 33.

is disclosed. In short, informational self-determination and consent both do not get much attention in the OECD Guidelines.

CoE convention 108 is also not based on the idea of information self-determination. The convention only mentions consent on just one occasion, namely in relation to the provision of possibility for assistance to data subjects that are residents abroad.[215] The convention further has no definition of consent. What the convention however does, contrary to the OECD Guidelines, is requiring a legitimate purpose and a lawful basis for processing.[216] This, arguably, is because the OECD is coming from an economical viewpoint, whilst the CoE convention 108, related to the ECHR[217], is coming from a fundamental rights viewpoint. According to Gonzalez Fuster the principles of convention 108 served as a basis for all subsequent European legislation.[218] Relating to this, it could be said that the DPD is influenced by national laws that utilized the consent of individuals, but also by this system of requiring a legitimate purpose and lawful basis. Arguably because of these influences, the DPD built a system where a lawful basis is needed, with consent being one of them.

4.2.2 The DPD and information self-determination

As stated by Mayer-Schönberger the DPD followed the evolution of data protection towards a system that protects the right to informational self-determination. According to Purtova, the directive's connection to privacy and other fundamental rights and interests of the individual expressed throughout the directive and its case law allows interpretation and implementation of the directive as an instrument implementing the right to informational self-determination.[219] Nonetheless, anchoring the principle into the DPD too strongly has not been possible. An example of this is the fact that German proposals for a default consent requirement for data processing were struck down by the UK.[220] It could however be argued that the DPD is in fact not based on but linked to the concept of information self-determination. This link between the directive and the principle of informational self-determination, or control of personal data by the individual, can be observed in the directive in a number of ways. A first obvious aspect of informational self-determination to be found

[215] Kosta 2013, p. 25.
[216] Art. 5 CoE convention 108
[217] The CoE conventions on data protection actually are an answer to the insufficiency of art. 8 ECHR in protecting personal data, see González Fuster 2014, para. 4.2.1.
[218] González Fuster 2014, p. 93.
[219] Purtova, *Computer Law and Security Review* 2013, no. 016/20013, p. 8. See also Purtova 2011.
[220] Purtova, *Computer Law and Security Review* 2013, no. 016/20013, p. 7.

in the DPD is consent. According to the directive consent is one of the possible ways of legitimizing data processing activities.[221] Furthermore, consent is required when personal is to be transferred to third countries outside of the EU that have no adequate level of data protection.[222] Consent in these cases can be seen as one of the most powerful ways of applying control to data processing activities. The reason for this is that the act precedes the data processing and it has the possibility of blocking the processing of personal data entirely (if the data controller of course finds no other legitimate ground that is). Next to this, the directive also grants other rights that relate to the right of informational self-determination, such as the right of access[223], the right of rectification[224] and the right to object.[225] These rights give individuals a certain degree of control. The right of rectification for example allows individuals to rectify, erase or block information that is incomplete or inaccurate and the right to object enables individuals to stop data processing in certain cases. The right of access is slightly different: this right could be seen as a right that is necessary to properly apply the other individual rights to control the processing of personal data.

Since the adoption of the DPD data protection for individuals has only increased in importance. This can be witnessed by consulting the EU Charter on fundamental rights. According to the charter, which became legally binding in 2009, there is a fundamental right to data protection.[226] In addition, in this same provision another change can be perceived. The charter specifically states consent as one of the legitimizing grounds for data processing, which arguably is suggesting consent has an important position in the data protection framework and control, the rationale behind consent, is therefore deemed important.[227]. However, it must also be mentioned that a proposal to formulate the right to data protection as a right to informational self-determination was rejected.[228] To conclude, the DPD shows an increased importance for user control or informational self-determination, but it does not seem to mean that it forms the core of data protection. This means that the directive does not acknowledge a formal right to information self-determination.

[221] Art. 7 DPD.
[222] Art. 26(1)(a) DPD.
[223] Art. 12(a) DPD.
[224] Art. 12(b) DPD.
[225] Art. 14 DPD. This right is also seen as an evident recognition of the right to informational self-determination according to Kosta et al 2011, p.84
[226] Art. 8 EU Charter.
[227] To compare: the other grounds are addressed as *"... or some other legitimate basis laid down by law"*.
[228] Peers et al 2014, p. 229.

4.2.3 The GDPR: enhancing user control

With the adoption of the GDPR the European data protection framework seems to be shifting more towards informational self-determination and granting individuals control over their personal data. Before the adoption of the GDPR, the Commission mentioned, after public consult, that citizens feel an increasing loss over their data.[229] In its "comprehensive approach on data protection in the EU" the Commission gave its ideas concerning individual control. In the Commission's view effective control is a precondition for individuals to enjoy a high level of data protection.[230] It therefore proposes to examine ways of clarifying and improving the rights related to control, such as the right of access, rectification, erasure or blocking of data. Moreover, the Commission wishes to complement the already existing rights with a right of data portability.[231] The importance of control is furthermore stressed in the regulation itself. In one of the first recitals it is stated that *"natural persons should have control of their own data*".[232]

A couple of new rights that the GDPR brings also add control for individuals. First there is the right to be forgotten.[233] Technically this is not a *new* right, as it was developed earlier in the Google Spain case of the CJEU. The right to be forgotten gives individuals in certain situations the right to obtain erasure of their personal data, such as when the individual withdraws his consent (which was the legitimizing basis of the data processing) or when the data are no longer needed in relation to the purpose for which they were collected or otherwise processed. Besides the right to be forgotten there is also the new right to data portability.[234] This right allows individuals, at their request, to receive from a data controller the personal data concerning him which he has provided to the data controller. Moreover, this information has to be given in a structured, commonly used and machine-readable format. According to Fialová the data portability should enlarge the informational self-determination of the individual, as it will be up to individuals to determine who will get access to data, for what purposes and for how long.[235] Van der Sloot mentions in this regard that it is clear that the philosophy behind this rule is that personal data should be controlled or perhaps even

[229] European Commission, 'Summary of replies to the public consultation about the future legal framework for protecting personal data', available at http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf, p. 21.
[230] COM (2010) 609 final, p. 7.
[231] COM (2010) 609 final, p. 8.
[232] Rec. 7 GDPR.
[233] Art. 17 GPDR.
[234] Art. 20 GDPR.
[235] E. Fialová, *Masaryk University Journal of Law and Technology 2014, Vol. 8:1, p. 46.*

owned by the individual.[236] Purtova, however, notices some anti information self-determination aspect of the right to data portability in its current form. According to her, the fact that the right can only be invoked in case the personal data is obtained by consent or by contract limits the right.[237]In addition, the idea that consent may not be used in situations of a clear imbalance between individual and data controller, limits the informational self-determination of individuals.[238] Finally, an increase in user control can be observed in the fact that already existing rights have been extended, such as the right to object and the right to resist automatic processing.[239] Extending these rights should mean improving control as well. These changes do however not mean that the formal right to informational self-determination is affirmed. Ensuring individuals control over their personal data is an important objective of the regulation, but this does not mean that is the core of data protection under the GDPR.

4.2.4 The GDPR and controller responsibility

The previous paragraph shows that user control is gaining importance in European data protection law. Another interesting development, however, is that responsibility of the controller is also gaining importance, in order to ensure a high level of data protection. The idea of controller responsibility can be observed in the data protection principles.[240] The principle of lawfulness for example provides data controllers a number of lawful grounds which require them to gauge the interests of individuals, whilst the principle of fair processing requires data controllers to take interests of individuals into account.[241] In the GDPR the idea of controller responsibility is enhanced because of the accountability principle and its accompanying mechanisms in chapter IV of the GDPR.[242] One thing that will increase controller responsibility is the provision which requires data controllers to take technical and organizational measures to implement data protection principles, protect individuals and to ensure that only necessary data is processed by default.[243] Furthermore, controller responsibility can be found in the fact that data controllers have to be transparent about data breaches[244], incentivizing them to avoid them, and in the fact that they are required to assess

[236] Van der Sloot, *International Data Privacy Law* 2014, Vol. 4/4, p. 315.
[237] Purtova, *Computer Law and Security Review* 2013, no. 016/2013, p. 16.
[238] Purtova, *Computer Law and Security Review* 2013, no. 016/2013, p. 14.
[239] Van der Sloot, *International Data Privacy Law* 2014, Vol. 4/4, p. 315.
[240] Quelle 2017, p. 5.
[241] Quelle 2017, p. 5.
[242] Quelle 2017, p. 5.
[243] Quelle 2017, p. 6. This rule is laid down in art. 25 GDPR.
[244] Art. 33 and 34 GDPR.

and find ways to mitigate high risks to the rights and freedoms of individuals.[245] In short, the task of data protection is, besides on individuals, also emphasized to be placed on data controllers.

4.3 Interim conclusion

The rationale of consent is related to the focus of data protection, which is information self-determination. The focus of data protection has however not always been like this. Initially data protection could best be described as a way to 'tame technology'. Later, due to technological and societal changes, this however changed, and data protection became more emphasized on protecting the privacy of individuals. This in turn ultimately evolved into the idea of informational self-determination. The main influencer of this development was the German Constitutional Court with its population census case in 1983. The principle of informational self-determination means that individuals should have control over the release and use of their personal data.

Over the years the informational self-determination has remained important. The DPD seems to have been somewhat inspired by it, as the DPD utilizes consent as an important way to legitimize data processing, and grants individuals a number of rights to control their data: the right to access data, the right to rectification and the right to object. With the coming of the GDPR the notion of informational self-determination seems to have become more important. This can demonstrated by all the signs of added control for individuals with regards to their own personal data. Furthermore, the Commission stated before drafting the regulation that control is necessary for individuals to enjoy a high level of data protection. Also, looking at the regulation itself the recitals themselves point towards the importance of individuals having control over their data. This importance is also reinforced by the fact that certain individual rights have been added or extended to provide for more control, such as the right to be forgotten or the right of data portability.

However, the increase of user control does not seem to mean that information self-determination is the core of data protection under the GDPR. One way to observe this is the fact that the regulation not only allows data processing to be done on the consent of individuals only, but on multiple lawful grounds. Furthermore, it can also be demonstrated by

[245] Quelle 2017, p. 6-7. The requirement can be found in art. 35 GDPR.

the fact that not only user control is important, but also controller responsibility. This last notion seems to have gained importance under the GDPR, due to the addition of the accountability principle and its accompanying mechanisms. In conclusion, information self-determination is not the core of data protection and whether this should or should not be so is debatable. In the end the question should be asked whether it is more important to give individuals the freedom to choose what is good for them, or if it is better to give them what is best for them. One thing important is that the critiques to information self-determination, privacy self-management or individual user control stated in the first chapter, cannot be ignored when answering this question.

5. Conclusion

The goal of this final chapter of this thesis is twofold. First, it is to summarize all main findings of the preceding chapters. Second, it is to discuss these findings in connection with the main research question, which is if the continued use of consent as a lawful ground for processing personal data in the GDPR can be explained by the rationale behind consent and the changes made to consent under the former DPD framework. Consequently, the main findings will first be discussed in this chapter, after which the main research question will finally be answered.

5.1 The main findings

According to the second chapter processing personal data is only possible when doing so in accordance with data protection principles and rules. One of those rules is that data processing should have a lawful basis, with consent being one of them. Next to stating the requirements for a valid consent the DPD is pretty silent on consent. By analyzing the current law concerning consent it has become clear that there is room for improvement. The DPD has still a lot to clarify, and its implementation is rather fragmented throughout the EU member states. The GDPR can help with is, as it can clarify consent and at the same time clear the harmonization problems as it is a regulation that does not need to be implemented because it has direct effect in each EU member state.

According to the third chapter one could conclude that the goals of both the DPD and the GDPR are the same. The aims of the DPD and the GDPR are twofold: ensuring a high level of data protection on the one hand and (by having a free flow of personal data) achieving an internal market within the EU on the other hand. Consequently, changes to consent should thus in general be seen as an attempt to strengthen the pursuit of these two aim, however with the emphasis on data protection. Moreover, the GDPR brings a number of changes to consent. First of all passive consent is effectively out of the picture, as the regulation states that affirmative action is required and silence, pre-ticked boxes and inactivity do not establish a valid consent. A second group of changes is about the freely given aspect of consent. According to the regulation consent should not be used in situations with a clear imbalance between the data controller and the individual. This could for example be government vs citizen, employer or employee or even some other relationship. Furthermore, consent is presumed to not have been freely given according to the regulation when the use of consent

for one processing activity is mandatory bundled with other processing activities or if consent is used for the performance of a contract, whilst the consent is not necessary for performing the contract. A third change is that "informed consent" is now clearer. Following the regulation, pre-formulated consent forms should be provided in easily accessible form and with clear and plain language. In addition, some topics the individual should always be informed about, such as the identity of the controller and the data processing purposes. Furthermore, in the case of online consent the request must be clear and not unnecessarily disruptive to the use of the service for which consent is asked. As a result of this, extremely long and vague privacy policies should no longer be allowed. A fourth change is the introduction of the right to withdraw consent. The right to withdraw itself actually not new, as it has been implied in the DPD, however the rule that giving and withdrawing consent should be of the same ease and without detriment is new. A fifth change is that, in line with the new accountability principle, data controllers are obligated to demonstrate the existence of consent. This means that evidence-gathering of consent becomes very important. Finally, a sixth change is that children under 16 require authorization of their legal representatives when asked for consent. In addition, data controllers have a new duty to verify the age of individuals to determine whether authorization is required. To summarize this research has shown that the GDPR adds new concepts, but mostly clarifies already known concepts. The GDPR has taken care of making the rules more harmonized and giving already known concepts (from for example the Working Party) a binding status.

Following the fourth chapter the rationale of consent seems to be related to the principle of information self-determination, which comes down to the idea that individuals should be able to control the release and use of their own personal data. This principle was made popular by the population census decision of the German Constitutional Court in 1983, after which it inspired European data protection law in some nations. Originally data protection started out as a means to tame technology, yet after a while because of changes in both technology and society it shifted more and more towards individual privacy and information self-determination. The relation between informational self-determination and the EU data protection framework can be observed by a number of things. The DPD for example uses consent as a lawful ground for processing and grants individuals with rights that grant them control over their data: the right to access data, the right to object data processing and the right to rectify data. In the GDPR this relation seems to be even stronger: the regulation itself mentions control as being important for individuals, it introduces new rights that improve

control such as the right to be forgotten and the right to data portability and it extends rights such as the right to object and the right to resist automatic processing. This does however not mean that there is a formal right to informational self-determination. Ensuring user control seems important, yet it is not the core notion of the GDPR.

5.2 Answering the research question

Following from the research done in chapter three it is apparent that consent has improved quite a bit. Long and non-understandable consent-requests should be a thing of the past, reducing the chance that people do not understand that which they consent to. Furthermore, consent cannot be used in situations anymore where there is a clear power imbalance between the data controller and the individual. Moreover, consent is presumed to not have been given freely when it is asked for services that actually do not need those data processing activities for which consent is asked. It can be argued that these changes reduce the amount of consents that will be made without a meaningful choice.

What has also become clear in chapter three, however, is that these improvements do not mean that consent in the future will be flawless. Instead, consent according to this research stays with a number of problems. Some of the problems mentioned by Solove will still remain. The problem of skewed decision due to individuals having a "bounded rationality" will still be present. Furthermore, the structural problems Solove mentioned, such as the problem of too many entities, the problem of aggregation and the problem of assessing future harm, will remain. Regarding these problems though, especially the changes concerning withdrawing consent, the right to be forgotten and the right to data portability can prove to be helpful in case a "wrong" data processing decision has been made by an individual. By exercising these rights an individual could easily remove the legitimizing ground and prevent future data processing, erase his or her past data and if desired take his or her data somewhere else.

Yet even if the system of consent in data protection law does still have flaws, it is not set in stone that consent should therefore be left behind. The reason for this is that according to chapter four the idea of informational self-determination or user control is regarded as an important notion in European data protection law, even if it is not the core idea of data protection. Besides, another argument to stick with consent would be that there are no better alternatives present at the moment that promote user control or informational self-determination like consent does. This is because all other legitimizing grounds in the DPD

and GDPR do not directly involve the individual in the decision whether data processing operations can happen or not. Furthermore, notwithstanding the question whether user control does or does not improve the level data protection of individuals, one must conclude that leaving consent would result in reducing freedom of individuals.

To summarize, the continued use of consent can be explained by the improvements to consent and the rationale of consent, which is the right to informational self-determination. However, the current system of consent still leaves room for improvement. The use of consent is not error free as there are still flaws to it, but newly added ideas in the GDPR such as the right to be forgotten and the right to withdraw consent as easy as it is given could help mitigate these problems with consent.

List of used literature and other sources

Articles

Acquisti & Grossklags, *IEEE Security & Privacy* 2005
A. Acquisti & J. Grossklags, 'Privacy and Rationality in Individual Decision Making', *IEEE Security & Privacy* 2005.

Bygrave, *Stockholm Institute for Scandinavian Law* 2004
L.A. Bygrave, 'Privacy Protection in a Global Context – A Comparative Overview', *Stockholm Institute for Scandinavian Law* 2004.

Fialová, *Masaryk University Journal of Law and Technology 2014, Vol. 8:1*
E. Fialová, 'Data portability and informational self-determination', *Masaryk University Journal of Law and Technology 2014, Vol. 8:1.*

De Hert & Papakonstantinou, *Computer Law & Security Review* 2016
P. de Hert and V. Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?', *Computer Law & Security Review* 2016/32.

Hornung & Schnabel, *Computer Law and Security Review 2009/25*
G. Hornung & C. Schnabel, 'Data Protection in Germany I: The population census decision and the right to informational self-determination', *Computer Law and Security Review* 2009/15.

Hull, *Ethics Inf Technol* 2015/17
G. Hull, 'Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data', *Ethics Inf Technol* 2015/17.

Hustinx, *Statewatch* 2013
P. Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', *Statewatch*.

Ilshammar, *Human IT* 2007, no. 9/1
L. Ilshammar, 'When Computers Became Dangerous: The Swedish Computer Discourse of the 1960s', *Human IT* 2007, no. 9/1.

Koops, *International Data Privacy Law* 2014
B.J. Koops, 'The trouble with European data protection law', *International Data Privacy Law* 2014.

Korff, *Londen Metropolitan University* 2010
D. Korff, 'Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments', *Londen Metropolitan University* 2010.

O'Neill, *Journal of Medical Ethics* 2003
O. O'Neill, 'Some limits of informed consent', *Journal of Medical Ethics* 2003.

Purtova, *Computer Law and Security Review* 2013, no. 016/20013
N. Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination Off the Table ... and Back on Again?', *Computer Law and Security Review* 2013, No. 016/2013.

Roßnagel, *Bundesministerium des Innern*
A. Roßnagel, 'Modernisierung des Datenschutzrechts', *Bundesministerium des Innern.*

Schermer, Custers & Van der Hof, *Ethics Inf Technol* 2014/16
B.W. Schermer, B. Custers, & S. van der Hof, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection', *Ethics Inf Technol* 2014/16.

Van der Sloot, *International Data Privicay Law 2014, Vol. 4/4*
B. van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation', *International Data Privacy Law* 2014, Vol 4/4.

Solove, *Harvard Law Review* 2013/1880
D.J. Solove, 'Privacy Self-Management and the Consent Dilemma', *Harvard Law Review* 2013/1880.

Solove, *University of Pennsylvania Law Review* 2006, Vol. 154, No. 3
D.J. Solove, 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* 2006, Vol. 154, No. 3.

Quelle, *IFIP AICT* 2017
C. Quelle, 'Not just user control in the General Data Protection Regulation' in A. Lehmann et al, *Privacy and Identity Management – Facing up to Next Steps*, Switzerland: Springer IFIP AICT 2017.

Books

Estabrooks 1995
M. Estabrooks, *Electronic technology, corporate strategy, and world transformation*, Westport: Quorum Books 1995.

González Fuster 2014
G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*', Switzerland: Springer 2014.

Handbook on European data protection law 2014
Handbook on European data protection law, Vienna: European Union Agency for Fundamental Rights 2014.

Kosta 2013
E. Kosta, *Consent in European Data Protection Law*, Leiden: Nijhoff Publishers 2013.

Kosta et al 2011
E. Kosta et al, 'Regulating Identity Management', in J. Camenisch, R. Leenes & D. Sommer, *Digital Privacy. Prime – Privacy and Identity Management for Europe*, Berlin: Springer 2011.

Kuner 2007
K. Kuner, *European Data protection law – corporate compliance and regulation*, Oxford: Oxford University Press 2007.

Luhmann 1965
N. Luhmann, *Grundrechte als Institution, ein Beitrag zur politischen Soziologie*, Berlin: Duncker & Humblot 1965.

Manson & O'Neill 2007
N. Manson & O. O'Neill, *Rethinking Informed Consent in Bioethics*, Cambridge: Cambridge University Press 2007.

Matzner et al 2016
T. Matzner et al, 'Do-It-Yourself Data Protection – Empowerment or Burden?', in S. Gutwirth et al, *Data Protection on the Move*, Dordrecht: Springer 2016.

Mayer-Schönberger 1997
V. Mayer-Schönberger, *Generational development of data protection in Europe*, Cambridge: The MIT Press 1997.

Moerel & Prins 2016
L. Moerel & C. Prins, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, Deventer: Wolters Kluwer 2016.

Peers et al 2014
S. Peers et al, *The EU Charter of Fundamental rights: A Commentary*, London: Bloomsbury publishing 2014.

Purtova 2011
N. Purtova, *Property rights in personal data: A European perspective,* Oisterwijk: BOXPress BV 2011.

Rouvroy & Poullet 2009
A. Rouvroy & Y. Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in S. Gutwirth et al, *Reinventing Data Protection?*, Dordrecht: Springer 2009.

Westin 1970
A. Westin, *Privacy and Freedom*, London: The Bodley Head 1970.

Case law

- BverfGE 65, 1 of 15 December 1983 (Volkszählung)

- CJEU, Joined cases C-465/00, C-138/01 and C-139/0, 20 May 2003 (*Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk*)
- CJEU, C-524/06, 16 December 2008 (Huber v. Germany)
- CJEU C-543/09, 14 October 2010 (Deutsche Telekom AG)
- CJEU, Joined cases C-468/10 and C-469/10, 24 November 2011 (*Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado)*
- CJEU C-131/12, 13 May 2014 (*Google spain*)

Other documents

- Article 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context'.
- Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability'.
- Article 29 Working Party, 'Opinion 15/2011 on the definition of consent'.
- Article 29 Working Party, 'Opinion 01/2012 on the data protection reform proposals.
- Article 29 Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC'.
- Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC.
- Article 29 Working Party, 'Working Document on the processing of personal data relating to health in electronic health records (EHR).
- European Commission, 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609 final.
- European Commission, 'Annex 2 - Evaluation of the Implementation of the Data Protection Directive', Annex to SEC (2012) 72 final.
- European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', COM (2012) 11 final.
- European Commission, 'Summary of replies to the public consultation about the future legal framework for protecting personal data', available at http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf
- European Data Protection Supervisor, 'Opinion on the data protection reform package (2012)'.