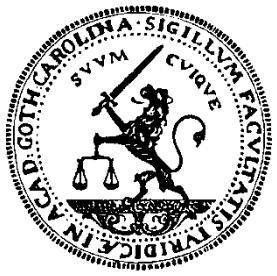

FACULTY OF LAW
Lund University

Milan Cobbaut

A Pound of Flesh

An examination of the scope of Directive 2019/770 and its notion of the data paying consumer in light of the GDPR

JAEM03 Master Thesis

European Business Law
30 higher education credits

Supervisor: Julian Nowag

Term: Spring 2023

Therefore prepare thee to cut off the flesh.
Shed thou no blood, nor cut thou less nor more
But just a pound of flesh: if thou cut'st more
Or less than a just pound, be it but so much
As makes it light or heavy in the substance,
Or the division of the twentieth part
Of one poor scruple, nay, if the scale do turn
But in the estimation of a hair,
Thou diest and all thy goods are confiscate

- William Shakespeare, The Merchant of Venice

TABLE OF CONTENTS

1. INTRODUCTION

Harmonised consumer protection in the digital sphere – Back in 1999, the EU legislature enacted the Consumer Sales Directive, which for the first time, harmonised the conformity requirements that consumer contracts on the sale of goods were subject to, as well as the remedies which should be applied in case of a lack of such conformity.[1] Twenty years later, the rules of this directive were updated and replaced in the new Sale of Goods Directive.[2] At the same time however, the legislature enacted another directive, which extended this protection against non-conformity into the digital sphere. The new Digital Content and Digital Services Directive[3] – the DCSD for short – was to be a part of the Union's Digital Single Market Strategy, which aims to remove barriers to trade between Member States in a digital environment, and thereby boost the digital economy of the Union as a whole.[4] A harmonisation of the rules on the conformity of contracts pertaining to the supply of digital content and digital services should make it easier for both consumers and traders to conclude such contracts across Member States borders, thereby strengthening the Single Market and further economically integrating the Member States.[5] In addition, these harmonised rules should help attain a high level of consumer protection, as is one of the EU's objectives per article 169(1) TFEU.[6]

The protection offered by the DCSD – The DCSD defines the concepts of digital content and digital services very widely. Any supply of 'data in a digital form' to a consumer will count as digital content provision under article 2(1) DCSD, while any service that allows consumers to interact with such data in some way, will be a digital service covered by article 2(2) DCSD. The former category should include all major streaming services – your Spotify and Netflix –, while the latter will encapsulate all social media platforms – Facebook, TikTok and so on. So simply put, when users of a streaming service or social media platform finds that what they are supplied, does not match the requirements of conformity described in articles 7 to 9 of the directive, they can invoke its remedies. In this regard, article 14(1) DCSD provides them with the option to have the digital content or digital service be brought back into conformity, or alternatively – under the conditions of article 14(4) and (6) DCSD – to demand a proportionate

[1] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L171/12
[2] Directive 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28
[3] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 (DCSD)
[4] DCSD, recital 1
[5] DCSD, recitals 3-7
[6] DCSD, recitals 2 and 8

reduction in the price they paid for it, or to terminate the contract in its entirety. Termination of the contract will result in a full reimbursement of the sums the consumer paid under it, in accordance with article 16(1) DCSD.

The scope of the DCSD – The DCSD principally only applies to contracts between traders – defined in article 2(5) DCSD as anyone acting for professional purposes – and consumers – which, according to article 2(6) DCSD, do not. While recitals 16 and 17 DCSD give the Member States, in transposing the directive, the option to expand its personal scope beyond consumers, it should be kept in mind that the DCSD is foremost an instrument of consumer law. The Member States retain a great deal of autonomy in general. Article 3(10) DCSD provides that all requirements of national law, specifically those relating to the formation and validity of contracts, continue to apply to contracts covered by the DCSD, as long as these national requirements are not regulated in the directive.

Data paying consumers – In addition to rules of national law, other rules of EU law will also continue to apply to contracts covered by the DCSD. Specifically, article 3(8) DCSD provides that the rules of data protection law, and then specifically those of the General Data Protection Regulation[7] – the GDPR for short – and the ePrivacy Directive[8] should be complied with for any data processing that occurs in connection with contracts covered by the DCSD, and that in case of conflict, these rules should take precedence over the DCSD. In this way, the directive alludes to one of its aspects that sets it apart from all other instruments of EU consumer law. Article 3(1) DCSD provides that, in order for a contract to enjoy protection under the DCSD, the consumer must pay – or undertake to pay – a price in exchange for the digital content or digital service concerned. This payment can be in money – including digital currencies, as article 2(7) DCSD makes clear – but rather uniquely, article 3(1) DCSD provides that such payment can also be made through the provision of personal data. As recital 24 DCSD makes clear, the legislature recognises that a significant percentage of traders supplying digital content and digital services, will do so for 'free', which actually means they do it in exchange for the personal data of the consumer. Instead of through paid subscriptions, these traders make a profit by extracting economic value from this personal data, e.g. by using it to enable targeted advertising. As the Commission stated in the original proposal for the DCSD, in a digital economy, personal data might be almost as valuable as money. Not including traders who employ a business model based on data gathering within the scope of the DCSD, would mean a large segment of the

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37

market – and thus a large group of consumers – would be exempt from the protection the directive provides. Not only would such amount to discrimination between consumers, it would also incentivise traders to require a payment in personal data over one in price, in order to avoid application of the DCSD's remedies.[9] Simply put, the inclusion of data providing consumers within the ambit of the DCSD's protection, is imperative to ensure that its provisions can be effectively applied in practice.

An analysis of GPDR concepts in a DCSD context – By introducing the notion of the data paying consumer in the DCSD, the legislature has allowed concepts traditionally reserved for data protection law, to be introduced and applied to a consumer law context. In this contribution, we will analyse two of these concepts, which are contained within the GDPR, and see what role they play in deciding how the scope of the DCSD should be interpreted, as regards data paying consumers. The first concept is that of 'personal data'. We will see what conditions data must comply with, in order for its provision by the consumer to lead to the DCSD's protection. It will become clear that, while interpretations coming from data protection law will have a significant impact here, the DCSD still sets up some requirements for personal data provision, which are distinct from those put forward by the GDPR. The second concept is that of 'consent' to data provision. We will see that the GDPR always applies to data provision under the DCSD, and that its requirements for consent must thus always be complied with. However, these requirements will clash with the very notion of a contract containing an obligation of data provision, which the DCSD provides for. Unlike what was the case for personal data though, the definition of consent to data provision, used to define the DCSD's scope, will be completely different from the one provided in the GDPR. However, the rules on the burden of proof regarding consent, will still play a role in applying the DCSD. This overview of these two concepts will first of all allow us to define under what conditions a consumer will have complied with a data provision obligation, which entitles them to protection under the DCSD. Secondly, it will enable us to assess the impact data protection law has on the scope of article 3(1) DCSD, as a provision of consumer law, and in what ways the collision between the two legal fields causes incongruences. Lastly, it will allow us to evaluate the legislature's endeavour to include the business model of data collection within the ambit of the DCSD, and analyse its shortcomings in doing so.

[9] Commission, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM (2015) 634 final, recital 13

2. PROVISION OF PERSONAL DATA IN THE DCSD

2.1. THE NEED FOR AN IDENTIFIED OR IDENTIFIABLE NATURAL PERSON

A link to data protection law – In its original Proposal for what was then still the Digital Content Directive, the Commission saw the notion of data paying consumer as quite an expansive one. The payment could be in 'personal' data, as well as in 'any other' data.[10] The scope seems to have been narrowed in the legislative process however, as in the final version of article 3(1) DCSD, only the provision of personal data, as defined in the GDPR, is taken into account. It should be noted in this regard that article 2(8) DCSD refers explicitly to the definition provided in article 4(1) GDPR. Therefore, the notion of personal data in the DCSD, and thereby the scope of the protection the consumer enjoys under it, is inextricably linked to the protection provided under data protection law.

Information relating to an identified or identifiable natural person – Article 4(1) GDPR's definition lays out several requirements for information to be personal data within its meaning. Firstly, it must be information 'relating' to a person, an element we will discuss further below. Secondly, this person must be a natural person. As the DCSD in principle only applies to consumers, defined in article 2(6) DCSD as natural persons acting in a non-professional capacity, this is of less practical importance to us here. Finally, this natural person must be able to be identified in some way. In the context of the DCSD, there are several ways in which such identification can be achieved.

Identification through account information – As explained by the Article 29 Working Party in its 2007 Opinion on the notion of personal data, there are different kinds of personal data, one of which is the kind that enables the identification of the subject it relates to. For data to be personal data within the meaning of the GDPR, it will always have to be somehow linked to other data that allows this person to be identified.[11] In the context of the DCSD, identification will usually be possible due to the fact that the data is attached to the account the consumer has with the trader providing them the digital content or services at hand. Indeed, recital 24 of the DCSD states that when the consumer gives their name and email address to the trader to open an account with them, such a situation falls within the directive's ambit.

[10] Ibid, art 3(1)
[11] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' WP 136 9-10

Identification through directly identifying metadata – Even when the consumer has never supplied any name and email address to the trader – or used ones that cannot be traced back to them in any way – it will in many cases still be possible to render them into an identifiable data subject. As elaborated upon by the European Data Protection Board in its 2020 Guidelines on targeting on social media, 'online identifiers' such as identifying cookies and IP addresses are often used by social media platforms to distinguish users and show them targeted advertising, even on isolated visits without a registered account.[12] The use of such online identifiers – including location data – has also been explicitly recognised in recital 30 GDPR. The DCSD is more ambivalent as to the use of these 'metadata' however, and then specifically as to whether they can be the object of a data provision contract within its scope, a discussion which we will delve further into down below. A differentiation should be made however between the metadata's role as personal data by itself, and its ability to convert other data into personal data by providing it a link to an identifiable person. Even if it cannot be the former under the DCSD, it should always be able to do the latter.

The subjective character of identifiability - When it comes to IP addresses, the Court of Justice has explicitly recognised their character as personal data under the GDPR, as they allow exact identification of the data subjects whose devices they are linked to.[13] In *Breyer,* it specified that this qualification not only applies to the classic 'static' IP addresses, which will always lead back to the same device over multiple browsing sessions, but can also extend to so-called 'dynamic' addresses, that are only used once and then discarded when the browsing session has been ended. The Court of Justice added however that these dynamic IP addresses will only count as personal data, when the data controller has access to the additional data required to make identification of the data subject possible.[14] This highlights the subjective character of the identifiability criterion: whether information counts as personal data – and thus can trigger both the GDPR and DCSD's protection – depends on what the data controller knows. Recital 26 of the GDPR recognises that when such data is of a pseudonymous nature, account should be taken of the means that the controller is reasonably likely to use, to be able to acquire the additional information necessary to link it to an identified natural person. The question to be examined is what linking information the controller could reasonably have access to, taking into account considerations such as the time and money that would need to be spent, as well as the technologies that are available to it now as well as in the foreseeable future.[15] The information

[12] European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' 7-8
[13] Case C-70/10 *Scarlet Extended* [2011] EU:C:2011:771, para 51
[14] Case C-582/14 *Breyer* [2016] EU:C:2016:779, paras 36 and 49
[15] GDPR, recital 26

possessed by third parties should also be considered, but only if there is a reasonable possibility that the controller could attain access to it, e.g. because it is easily findable online.[16]

Identification through tracking the overall online behaviour of the data subject – Lastly, identification of the consumer-data subject can also be possible through the data they provide by interacting with the digital content or services. Recital 24 of the DCSD mentions the uploading of photographs and posts to the trader's digital service as an act of personal data provision that can induce the DCSD's protection. The Court of Justice elaborated upon this further. In *Buivids*, it stated that the fact that the data subjects could be seen and heard on the recorded video footage, sufficed for this footage to be qualified as personal data linked to an identifiable data subject.[17] Presumably, this means that any picture, audio or video consumer upload, in which they can be seen or their voice can be heard, could be enough for them to be identifiable and count as data paying consumers. Article 4(1) GDPR also acknowledges the possibility of identification of a data subjects through their physical characteristics, as well as through any economic, cultural or social ones. Of course, once again the identifiability is dependent upon the information the traders-controllers has reasonable access to, e.g. whether they can reasonably link the voice heard in a video to a distinguishable data subject. The means available to the providers of digital content and digital services should not be underestimated though. Through tracking a person's online presence – what they upload, like or click on –, they will often be able to create a distinguished and thus identifiable data subject, defined by a unique amalgamation of interests, behaviours and attributes, without ever needing to know their name.[18] This practice is recognised by article 4(4) GDPR as 'profiling'.

2.2. DATA RELATING TO THE CONSUMER

Data 'about' a person – According to the definition provided in the GDPR – and referred to in the DCSD – information will only be recognised as personal data, when it 'relates' to the concerned data subject – in casu to the consumer consenting to data provision under the DCSD. In its Opinion on the definition of personal data, the Article 29 Working Party clarified that it is simply required that the information at hand is 'about' the data subject in some way. Data that allows the data subject to be identified, either directly or indirectly, will therefore always be personal data within the GDPR's ambit, as it gives information 'about' him, specifically their identity. A second kind of personal data should be distinguished however, namely that of information that provides insights into the data subject's characteristics or behaviours, without

[16] Paul Voigt and Axel vom dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017)
[17] Case C-345/17 *Buivids* [2019] EU:C:2019:122, paras 31-32
[18] European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' 9

them being identifiable through this information by itself. Such data will however only be personal data, if it is somehow linked to other data that makes identification possible. The Article 29 Working Party gives the example of performance evaluations in a company's employee database. How the employee performed, is indeed information relating to him, as it reflects their behaviour and characteristics. It is however only personal data, because it is linked to identifying information, i.e. their name at the top of the page. In this regard, it should be noted that the potential use of the data can also have an impact on its classification. The Article 29 Working Party notes that when information can be used to evaluate the data subject, or otherwise influence their status, behaviour, or how they are treated, such information should be seen as personal data that enjoys protection under the GDPR. It will qualify as information 'relating' to a data subject, even if the information was not gathered for evaluative purposes. The possibility of evaluation or influence seems to suffice.[19]

User-generated content as personal data – When consumers enters into a data provision contract covered by the DCSD, they can fulfil their data provision obligations immediately, e.g. by making an account and thereby providing information like their name and email address to the trader. Alternatively, they can choose to provide their data at a later time, after the conclusion of the contract. As article 3(1) DCSD puts it, it suffices that the consumer 'undertakes' to provide personal data when they conclude the contract. Recital 24 of the DCSD explicitly recognises the possibility of data provision after the contract's conclusion, specifically through the content the user creates and shares while enjoying the trader's digital content or digital service. Indeed, aside from account information and tracking through metadata, analysis of the content the consumer generates using the digital content or service, will be the main way in which the trader will gather personal data.

Pictures, audio and video as personal data – We already mentioned that the pictures, audio and video the consumer uploads can often be categorised as personal data, because they will contain their voice or appearance, and thereby allow them to be identified. But even when the footage at hand only concerns certain objects or events, without directly showing the consumer, they will often still be 'about' them in some way. For instance, the fact that the consumer owns the object, or that it has some sort of influence on them, or just simply the information that they were once physically close enough to it to take a picture of it, all reveal something about their behaviour and characteristics.[20] For similar reasons, footage only containing other people can still provide information about the consumer in some way, and thus still be 'about' him. Even when it does not relate to themselves however, but to other people, the footage might still

[19] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' WP 136 9-11
[20] Ibid 9

invoke the DCSD's application. Strictly speaking, article 3(1) DCSD does not specify anywhere that the data the consumer provides to the trader, must be their own personal data. Presumably though, the idea of deliberately exchanging other people's data for access to digital content and services does not align well with the spirit of the directive, as it raises some privacy concerns.

Other kinds of user-generated content – Clearly, the notion of data 'about' a person, can be interpreted quite extensively in the context of user-generated content. For instance, almost any text post consumers make using the trader's services, will reveal something about their personality, opinions or actions, and will thus be information relating to them. Similarly, any like or rating they give, or playlist they make or share, will reveal their preferences. As recital 28 DCSD makes clear, also information found in email and online messaging services the consumer uses, should be included. Everything the consumer creates, uploads or shares on the trader's platform, reveals something about their identity, characteristics, and behaviours, and can be used to profile, evaluate and influence him, i.e. through targeted advertising. Not only will all this user-generated content relate to him, it will also make them identifiable. As discussed above, even when the provided information cannot be connected to an account, IP address or identifying cookie, identification will still be possible through collecting all the by itself behavioural data – i.e. through providing user-generated content – and combining them to create a unique profile. As the European Data Protection Supervisor recognised in its opinion on the DCSD's original proposal, almost all of the information the consumer will provide to the trader, will count as personal data within the scope of the DCSD.[21] In fact, it argues that the simple fact that the consumer has actively created the user-generated content in question, implies that it relates to him.[22] Therefore, the special rules regarding further use and retrieval that article 16(3) and (4) DCSD have worked out for user-generated content that does not qualify as personal data, will arguably be of little importance in practice.

2.3. EXCLUDED PURPOSES: A NOTION OF ECONOMIC VALUE

The purpose of data collection – Article 5(1)(b) GDPR provides that the processing of personal data is only allowed, if it has a specified and legitimate purpose, and only to the extent that such is compatible with this purpose. This idea of purpose limitation is one of the fundamental principles of the GDPR. Therefore, any analysis of data processing under the GDPR should include an examination as to why the controller wants the data in the first place. Under the DCSD, the purpose the trader has for the data provided by the consumer will also have to be considered. If they need the data exclusively for one of the purposes specified in article 3(1)

[21] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 11
[22] Ibid, fn 47

DCSD, the contract will not fall within the scope of the DCSD, and the data providing consumer will not be able to benefit from its protection. However, if the data collection has more than one purpose, or if the data is later processed for other purposes, and these additional purposes are different from the ones listed in article 3(1) DCSD, the contract will still be within the DCSD's ambit.

Excluded purposes – Article 3(1) DCSD distinguishes two purposes the trader could have for collecting personal data, which, when linked to the data provided by the consumer, could lead to exclusion of the data provision contract from the DCSD's scope. First off, the DCSD will be rendered inapplicable, if the trader needs the data to comply with the legal obligations they are subject to. In this regard, the DCSD seems to particularly point towards registration and identification requirements member states might impose on providers of digital content and digital services, out of national security concerns.[23] Secondly, data provision will not invoke the DCSD's protection, if it is simply necessary for the trader to provide the consumer with digital content or digital services which comply with the requirements laid out by the contract and the conformity requirements of the directive itself. In its original proposal, the Commission gave the example of the collection of geographical location data needed to ensure the proper functioning of a mobile application[24], but this was omitted from the definitive version of the directive. But for instance, the collection of the address or email address of the consumer, so the digital content can be delivered to him, could be data provision necessary for the performance of the contract. Similarly, when the consumer provides the trader with their credit card details – which are necessary to ensure payment for the digital content and services –, this should be excluded from the directive's scope.[25]

Interpretation in light of the GDPR – It must be noted that the two excluded purposes in article 3(1) DCSD share a striking resemblance to two legitimate grounds for processing provided for in article 6 GDPR. It therefore stands to reason that the conditions under which these grounds can be relied upon, should also be relevant in determining those under which the excluded purposes will be relevant in the DCSD. First of all, the exclusion of data necessary to provide the digital content or digital service in question, seems to correspond to the ground in article 6(1)(b) GDPR, which concerns data processing necessary for performance of a contract. The Article 29 Working Party has clarified that this ground – and thus here, this exception – cannot be relied upon for every data provision that is covered by the contract in question. For instance, the fact that the contract explicitly allows the trader to engage in profiling activities,

[23] DCSD, recital 25
[24] Commission, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM (2015) 634 final, recital 14
[25] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' 10

will not suffice for the exception to be relied upon. If the trader has not been contracted by the consumer to do such profiling for them - i.e. the profiling is not a part of the digital content or digital services that are being supplied, then it will not be deemed necessary for the contract's performance.[26] Secondly, the exception corresponding to a legal obligation the trader might have, can be found as a legitimate ground for data processing in article 6(1)(c) GDPR. In this regard, the Article 29 Working Party has explained that, for this purpose to be relied upon, the trader must truly have no choice but to comply with the obligation. If they had a choice whether or no tot comply, or has a lot of discretion as to how to go about such compliance – i.e. because the obligation is not sufficiently clear and specific –, this exception will not be deemed applicable.[27]

The economic value of the data – The question must be raised as to why the legislature chose to deny protection to certain data provision contracts, simply because of the reason why the trader wants the data. After all, from the consumer's point of view, this is not of the most importance. Their purpose for providing the data is the access to digital content and digital services in return. The motivations the trader has for asking the data do not change this, either way they will have given up their personal data, and thereby some of their privacy. Clearly, when drafting the DCSD, the legislature did not solely have the best interests of the consumers at heart. By adding in the necessity exception in article 3(1) DCSD, it wanted to ensure that only situations in which the trader has some additional use for the data, beyond the mere fulfilment of its contractual and legal obligations, would be included within its scope. In this regard, it should be noted that the DCSD applies to traders, i.e. persons acting for professional purposes. So while it is definitely possible for the trader – specifically when it concerns a government-owned business – to also have some more altruistic or public interest purpose for the data collection at hand, in the vast majority of cases, they will want the consumer's data because they can make money off of it in some way. For instance, as we already discussed, they can combine the personal data they have about the consumer to create an accurate reflection of their socio-economic and demographical characteristics, as well as their interests and preferences. Subsequently, they can use these techniques to charge advertisers more per ad on their digital content or service, under the promise that the ads will be targeted towards the groups they will be the most effective on.

Personal data collection as a business model – The idea that personal data should have some economic value to the trader, for its provision to trigger the DCSD's protection, is also reflected

[26] 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' WP 217 16-17
[27] Ibid 19

in the DCSD itself, beyond the necessity exception in article 3(1) DCSD. Recital 24 DCSD recognises the importance of data collection as a business model for traders, and explicitly names the processing of user-generated content for marketing purposes, as a situation which should lead to the directive's application. Additionally, the very fact that data provision is included in article 3(1) DCSD as the alternative of paying a 'price', i.e. something have a monetary value, also point to the economic logic that seems to be behind the inclusion of data provision contracts within the DCSD's scope. In its opinion on the initial Commission proposal for the DCSD, the European Data Protection Supervisor affirms this in no uncertain terms. It states that the directive is meant to recognise the economic model in which providers of digital content and digital services collect personal data in order to create value with them. This is why services that are seemingly 'free' – but actually require provision of personal data – are included within its scope.[28]

The economic value of consent – In this context, it should also be noted that the economic value the trader gets from personal data provision, does not necessarily come just from the fact that the trader is receiving the personal data from the consumer. After all, there are many options for tech companies to attain a consumer's personal data. Often times, they will already have access to it, before any contract has even been concluded. The real value lies in the fact that they are usually getting the data with the consent of the consumer, and then specifically consent to process for certain further purposes that allow them to profit off of it in some way.[29] We will discuss below that consent under the DCSD does not necessarily have the same meaning as is ascribed to it under the GDPR, and is not subject to the same requirements. However, seeing the importance that receiving consent under the GDPR has in the business model of the trader, they will likely try to meet the GDPR requirements anyway.

The unfairness of a requirement of economic value – In essence, the DCSD seems to suggest that, besides meeting the requirements the GDPR posits, the personal data provided must have some sort of economic value for the trader, for the consumer to be able to benefit from the DCSD's provisions. Presumably, this means that if the trader can prove they did not profit from the provided data concerned in any way, beyond the purposes enumerated in article 3(1) DCSD, they will be able to escape the application of the DCSD, and thereby accountability for the lack of conformity they are responsible for. This does not seem to be fair on the consumer however. After all, it can be hard for them to distinguish what purposes the personal data they have provided, will be used for, and under what circumstances this will lead to them losing access to

[28] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 7
[29] Carmen Langhanke and Martin Schmidt-Kessel, 'Consumer Data as Consideration' [2015] Journal of European Consumer and Market Law 218, 220

the remedies the DCSD provides them with. Moreover, this means the trader is incentivised to hold back information on the purpose of the processing – even though such would be contrary to their information obligations under the GDPR – in hopes of making the consumer falsely believe there is no legal recourse available to them under the DCSD. In general, as we pointed out above, it is unclear why the consumer should care whether the trader makes money off of their data, as this does not impact the fact that they have made a payment, through sacrificing some of their privacy. Consequently, the notion of 'value' should perhaps be seen from the consumer's perspective, instead of from that of the trader. It would be unfair to exclude a consumer from protection under the DCSD, even though the data provision has cost them something valuable, namely their privacy.

Economic value beyond personal data – The economic value requirement, despite being not entirely fair and transparent from the consumer's point of view, still has strong support in article 3(1) DCSD, as it is essentially at the core of that provision's necessity exceptions. Therefore, attention should be paid to the fact that it could also benefit the consumer in some ways, namely by exposing the relative arbitrariness of the above discussed requirement that the data provided be personal data within the meaning ascribed by the GDPR. After all, it is feasible that traders could extract economic value from data provided by the consumer, even when the consumer cannot be identified, e.g. because the trader anonymises it immediately and only uses it in aggregated form. It would therefore be unfair on the consumer to deny them the remedies provided by the DCSD, just because the data they provided was only used by the trader in anonymised form. If the trader has made a profit from its use, the consumer should be entitled to protection under the DCSD, regardless of the nature of the data they have provided.[30] A similar case can be made for the copyright that exists on the content the user generates using the trader's digital content and services. Following the logic behind the economic value requirement, it would make sense that the transfer of such copyright to the trader could suffice as counter-performance for access to the trader's digital content and digital services.[31] After all, this copyright, as an intellectual property right, has a real economic value to the consumer, and potentially also to the trader. Perhaps the rules on the further use and return of user-generated content that is not personal data in article 16(3) and (4) could be applied to the copyright on the content, and thus still find some practical use.

[30] Zohar Efroni, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' [2020] Common Market Law Review 799, 810-811

[31] Vanessa Mak, 'The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content' (Workshop for the JURI Committee 2016) 10 <https://op.europa.eu/en/publication-detail/-/publication/6cfb903b-c295-11e6-a6db-01aa75ed71a1> accessed 21 April 2023

Alternative instead of cumulative application – So both the requirement that the data provided should be personal data, as the requirement that it should have some economic value for the trader, exclude certain situations from the protection of the DCSD, in ways which are unfair to the consumer to some extent. A solution would be to render these conditions alternative rather than cumulative. Data would then be covered by the DCSD, if it either had privacy-related value to the consumer, or economic value to the trader.

Abolition of any requirement of counter-performance - However, there are also some general objections of a philosophical nature of reducing personal data to what economic value it has. As pointed out in recital 24 DCSD, the protection of personal data is a fundamental right, and thus personal data should not be seen as a commodity. This sentiment is echoed by the European Data Protection Supervisor in its opinion on the DCSD's original Commission proposal.[32] Therefore, it suggested to abolish any notion of the requirement of a counter-performance on the consumer's end. It takes inspiration from article 3(2)(a) of the GDPR, which makes clear that the GDPR apples to data processing in the context of goods and services, regardless of whether any payment is required.[33] Alternatively, it suggests to keep a requirement of remuneration of some kind, but to stop requiring that this should come directly from the consumer. It refers back to the case law European Court of Justice concerning the interpretation of the freedom to provide services ex art. 57 TFEU, which allows for the remuneration to be performed by third parties.[34] In the context of the DCSD, this remuneration would then be made by the third parties – e.g. advertisers – who help the trader extract economic value from the data.[35] A wider interpretation of the DCSD's scope would in any way prevent the arbitrary nature of the scope of the protection the consumer is now subject to, and it is therefore regrettable that the legislature did not follow the European Data Protection Supervisor's advice.

2.4. MIXED CONTRACTS

Mixed payments – Article 3(1) DCSD seems to frame the act of provision of data as a strict alternative to a more conventional payment in the form of hard currency: either you pay in money, or in data. While, as the European Data Protection Supervisor reiterated in its opinion on the DCSD's original proposal, the inclusion of data provision contracts within the DCSD's field of application is indeed motivated by concerns around so-called 'free' services[36], the concept of

[32] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 7
[33] Ibid 10-11
[34] Case 352/85 *Bond van Adverteerders v State of the Netherlands* [1988] EU:C:1988:196, para 16
[35] Ibid 10
[36] Ibid 7

data provision contracts under the DCSD should be interpreted more broadly. Indeed, in many cases the payment the consumer makes to the trader will be of a mixed nature, and thus involve both money and personal data. To ignore this reality, would undercut the directive's aim to comprehensively target all traders implementing a business model based on the collection of personal data.

Payment information – It is possible that, by the very act of paying for a digital content or digital service, the consumer will, besides currency, also be providing the trader with their personal data. The most obvious example here is credit card information the consumer will provide the trader to ensure payment is possible. Of course, as long as the trader uses this information solely for in order to process the payment, it should be classified as data provision necessary to provide the digital content or digital services, and thus be covered by the exception to the DCSD's scope provided by article 3(1) DCSD. However, the trader could feasibly also use this payment information for additional purposes, e.g. in order to link certain behavioural data back to an identifiable natural person, and thereby create a profile of a person which can be used for targeted advertising. In such a case, the transfer of the payment information will not be covered by the exceptions in article 3(1) DCSD. It can thus be seen as a provision of information relating to an identified or identifiable natural person as defined in the GDPR, which also has some economic value to the trader. Simply put, by paying with a currency, the consumer is indirectly also paying with data.

Digital representations of value – Article 2(7) DCSD provides that payments in price – i.e. payments not in personal data – could be in conventional currencies, or alternatively, using a 'digital representation of value'. Recital 24 of the DCSD understands such to include i.a. electronic vouchers and coupons, but also virtual currencies, so long as these are recognised as a valid form of payment for services under Member State law. This seems to be an attempt of the legislature to future-proof the DCSD. Recital 24 states that the directive aims to acknowledge the rise of digital payment methods in the context of the supply of digital content and digital services. By including these payment methods within its scope, it wants to ensure that traders will not try to evade the application of the directive, by only allowing consumers to pay through digital means.

Virtual currencies – While the DCSD does indeed recognise the potential use that digital payment methods could have in the future economic landscape, it fails to account for the data gathering possibilities these novel methods, and then specifically virtual currencies, represent. We will not go into the intricacies of how the blockchain system which allows a decentralised system of virtual currencies to function, works. For our purposes, it suffices to mention that

when a consumer pays a trader in such a currency, the trader can trace this transaction back to an address. If the consumer used a static address – which is unchanging, and used for multiple transactions the consumer enters into – this will render them identifiable to the trader. Subsequently, the trader can easily check for which other goods and services the consumer has paid using this address. This reveals information about their spending habits, which the trader can then utilise for the purpose of targeted advertising, and thus allows them to extract economic value from it. Therefore, a payment through a virtual currency using a static address, can also easily meet the requirements for data provision contracts under article 3(1) DCSD. Even when the consumer employs a so-called 'shadow address' to pay the trader, which are one time use and obscure the static address – there will often times be ways for the trader to link this shadow address to other payments made by the same consumer, and allow them to single out an entity to which certain behaviours, preferences and characteristics can be ascribed. It should however be mentioned again here that identifiability is subjective. The information hiding behind the shadow addresses will only be classified as personal data covered by the DCSD if the trader has access to the extensive means required to enable identification. However, in this regard, the data gathering industry should not be underestimated.[37]

Priority of the classification as 'price' – So we have established that any payment using either conventional or digital currencies, could be accompanied by a data provision that meets the requirements of article 3(1) DCSD. However, such should not take away the fact that these contracts should be principally seen as involving a payment of a price. After all, if priority is always given to the fact that data is being provided, this might take away from the purpose of the DCSD's provisions relating to consumers who paid in hard currency. Specifically, the situation should be avoided in which the consumer is denied certain remedies reserved for price paying consumers, because this classification is ignored in favour of their status as a data paying consumer. Article 14(5) DCSD offers the consumer a proportionate reduction in price as a subsidiary remedy, in case a lack of conformity that cannot or will not be addressed of by the trader, has been established. Similarly, article 16(1) DCSD entitles the consumer to a full reimbursement of all amounts paid, in case the contract is terminated. The consumer will be deprived of these rights, if they are only seen as a data paying consumer. After all, the directive does not provide for similar remedies for reduction and reimbursement of payment in data. Not only because personal data is not quite as easily countable as a payment in currency is, but also because a reimbursement of data does not undo the initial provision of it in the same way as it does for payments in currency. Of course, article 17(1) GDPR provides the data subject – here the consumer – with the right to ask for the erasure of the personal data, if they withdraw their

[37] Michèle Finck and Frank Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' [2020] International Data Privacy Law 11, 29-31

consent to data processing or if the data is no longer necessary for the original purpose of the processing. Additionally, article 15 GDPR provides them with a right to access the data they provided, and article 20 GDPR with a right to receive and transfer it. However, as article 7(3) GDPR puts it, after the withdrawal of consent, all the data processing operations that happened before it, remain lawful and can thus not be undone. Indeed, unlike a repayment of money, the restitution of data does not undo the economic value the trader already has been able to extract through the processing it has already done, nor will it change the fact that the consumer's privacy has been infringed upon in this way. So the remedies involving reduction or reimbursement of payment are only really available to price paying consumers, and should not be ignored by prioritising the act of data provision which accompanies the payment of the currency. However, it can also not be forgotten that data provision has taken place. The protection offered by the GDPR – which is, according to article 3(8) DCSD, always still applicable to contracts covered by the DCSD – should still remain available to the consumer. Specifically, as article 16(2) DCSD provides, all the obligations which spring from the termination of the contract, imposed by the GDPR, should still be complied with.

Different consumer expectations – So a classification as a price paying consumer offers more protection to the consumer than one as a data paying consumer, because the DCSD offers them additional remedies as a price paying consumer, without depriving them of the remedies data protection law offers the data provision aspect of their payment. Aside from this, this classification is also to be preferred, because the bar for what counts as a lack of conformity – which entitles the consumer to the DCSD's remedies – might be lower for payments in price than it is for those in data, thereby granting more extensive protection to price paying consumers. The requirements in article 8(1)(b) DCSD make clear that the assessment of – a lack of – conformity must take into account the expectations the consumers may reasonably have for the quantity, qualities and features of the digital content of digital services. It stands to reason that when the consumer perceives the digital content or digital service to be 'free', because it only requires a – not always well signalled – provision of personal data, this might impact what they expect to be provided with. Specifically in cases where there is a 'free' version of the digital content or digital service, which is opposed to a paid version with additional features, their expectations as to the functioning and quality of the digital content or digital service, might be lower for the former, than for the latter. Consequently, the conformity requirements might be interpreted less strictly for 'free' digital content and digital services – whose business model is actually based on the collection of personal data - which means the consumer will receive less

protection, than they would for a paid service.[38] So following this reasoning, the fact that the consumer paid a price should be prioritised over the personal data provision that may have occurred in the process, to ensure their effective protection. It should however be noted that this reasoning is only based on an assumption, and that there is at least one empirical study which disputes it. The study in question concluded that, while the surveyed consumers might still report some kind of difference in expectations based on whether or not they have to pay hard currency for access to digital content or digital services, this difference should not be large enough to have a real impact on the interpretation of the conformity requirements the DCSD puts forward.[39]

Separate payments of price and data – So far we only paid attention to situations in which the payment of price and personal data the consumer has effected in exchange for access to digital content or digital services, are intertwined, and thus simultaneous. This situation of mixed payments must be differentiated from that of contracts which involve separate payments of data and price. A prominent example is that of so-called 'freemium' games, where the original download is 'free of charge' – and actually entails a provision of personal data to the trader – but a payment in money will be required in order to access additional perks, levels or features. Presumably, there are two separate contracts here, both covered by the DCSD. There is one contract that is concluded when the consumer first downloads the free version of the game, and is subject to the rules applicable to data paying consumers. A second contract will then be brought into being when the consumer pays for the additional features, and will entitle them to the additional remedies and stricter conformity assessment enjoyed by price paying consumers. However, this idea of separation into two different contracts might be hard to apply in practice, as it might be difficult to distinguish when a conformity problem is to be assessed using the expectations reasonably held by data paying consumers, and when it instead has to be based on those who paid a price.[40] In any case, as soon as a lack of conformity in the 'free' part of the digital content or digital service, negatively affects features which have been paid for, the consumer should be entitled to the remedies specifically available to price paying consumers. So for instance, when the game is overall malfunctioning and unplayable, the consumer should be able to – as a subsidiary remedy at least – get back the money they paid for a character costume, which they can no longer enjoy due to this malfunctioning.

---

[38] Marco Loos, Natali Helberger, Lucie Guibault and Chantal Mak, 'The Regulation of Digital Content Contracts in the Optional Instrument of Contract Law' [2011] European Review of Private Law 729, 757

[39] Madalena Narciso, 'Consumer Expectations in Digital Content Contracts – An Empirical Study' (2017) Tilburg Private Law Working Paper Series 1/2017, 19 <https://ssrn.com/abstract=2954491> accessed 9 April 2023

[40] Madalena Narciso, ''Gratuitous' Digital Content Contracts in EU Consumer Law' [2017] Journal of European Consumer and Market Law 198, 205-206

2.5. THE SPECIAL CASE OF METADATA

The evolution of the scope of the DCSD – The final version of article 3(1) DCSD, differs in many ways from the original Commission proposal. For instance, the wording that the provision of personal data is a 'counter-performance' for the supply of digital content or digital services[41], has been scrapped in the legislative process, presumably after the European Data Protection Supervisor recommended such in order to de-emphasise the transactional nature of data provision contracts.[42] Other changes had a more substantial impact on how the scope of the DCSD should be interpreted though. We already mentioned how the proposal originally allowed consumers to provide any data to enjoy protection under the DCSD[43], and that this was later narrowed down to data which qualifies as personal data under the GDPR, instead. In another way, the Commission proposal defined the scope of the DCSD more restrictively than the final version though. Specifically, article 3(1) of the proposal provided that data provision could only lead to application of the directive, if the consumer provided the data 'actively'. What active data provision exactly entails, is not defined in the provision however. Recital 14 of the proposal gives us a clue though: when the trader collects the information through the use of IP addresses and cookies, such does not qualify as active data provision.

The exclusion of metadata – Following criticism by the European Data Protection Supervisor in its opinion on the DCSD's proposal, the requirement that the data should be provided 'actively',[44] has been omitted from article 3(1) DCSD. However, this does not necessarily mean that all personal data collected through the use of cookies and IP addresses, is now covered by the DCSD. Recital 25 DCSD namely provides that when the trader only collects metadata from the consumer, this is in principle not enough to lead to the DCSD's application, unless Member State law provides otherwise. It should be noted however that what data is excluded, is no longer defined by the – passive – method through which it is collected, namely through the use of cookies and IP addresses. Instead, the emphasis is now on the kind of data that the trader can collect using these methods, i.e. metadata. Metadata is traditionally described as 'data about data', such as where, how and by whom the data was created.[45] Recital 25 DCSD gives two main examples of what it considers to be metadata. On the one hand there is information relating to

[41] Commission, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM (2015) 634 final, art 3(1)
[42] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 9-10
[43] Commission, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM (2015) 634 final, art 3(1)
[44] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 12
[45] Madalena Narciso, ''Gratuitous' Digital Content Contracts in EU Consumer Law' [2017] Journal of European Consumer and Market Law 198, 207

the device the consumer uses to access the digital content or digital service, and on the other there is information relating to their browsing history. As we will discuss below, both these types of information meet the requirements for personal data provided by the GDPR. So if the DCSD were indeed to exclude them from its application, that would mean it uses a notion of personal data which diverges from the one in the GDPR.

Device-related metadata as personal data –We established above that traders can use IP addresses and information gained through identifying cookies to render consumers into identifiable data subjects, even when they have not created an account with the digital content or digital service they offer. This role is also explicitly recognised in recital 30 GDPR. As information that identifies a natural person, is necessarily also information 'relating' to this person, their collection must be seen as processing of personal data as defined in the GDPR. Regarding IP addresses, the Court of Justice also confirmed their status as personal data in *Scarlet Extended.*[46] In *Breyer*, it extended this classification to IP addresses that had undergone pseudonymisation, provided that the data controller could reasonably access additional information that would allow for identification of the relevant data subject.[47] What concerns identifying cookies, the Court of Justice elaborated upon their status in *Planet49*. It stated that, by sending and recollecting a cookie containing a specific number to the device of the data subject, which it could then use to identify him, the data controller in question engaged in the processing of personal data.[48] It should be noted that this case did not concern the interpretation of the GDPR, but instead personal data processing under the ePrivacy Directive.[49] However, the directive is meant to complement the general rules on data protection rules, as found in the GDPR, and provides more specific rules applicable to personal data processing in the electronic communications sector.[50] Moreover, the notion of personal data is to be interpreted in the same way.[51] Therefore, as the Court of Justice makes clear,[52] the different instruments have to be read in conjunction, and thus the *Planet49* judgment is also relevant in a GDPR context. To conclude, the use of cookies and IP addresses by a data subject to single out a data subject's device, and thereby also identify the data subject, should be seen as processing of personal data within the meaning of the GDPR.

[46] Case C-70/10 *Scarlet Extended* [2011] EU:C:2011:771, para 51
[47] Case C-582/14 *Breyer* [2016] EU:C:2016:779, paras 36 and 49
[48] Case C-673/17 *Planet49* [2019] EU:C:2019:801, para 45
[49] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37
[50] Ibid, art 1(1)-(2)
[51] Ibid, art 2
[52] Case C-673/17 *Planet49* [2019] EU:C:2019:801, para 65

Tracking metadata as personal data – In its guidelines on targeting on social media, the European Data Protection Board recognised that one of the ways in which traders may collect personal data about a data subject, is through tracking their online behaviour. By keeping track of things such as what pages the data subject has visited, what links they have clicked on, how much time they have spent on each page, or what they type into the service's search bar, the trader can infer information about their preferences and characteristics, which can then be used for targeted advertising.[53] As we already discussed, in the modern data collection industry, traders will often have the ability to single out an identifiable natural person that advertising can be targeted towards, purely based on a unique combination of behaviours, preferences and characteristics.[54] Tracking the user's browsing activity can thus be a useful tool in this. Even when it does not enable identification though, the data subject's browsing behaviour will still be information 'relating to him', so – as long as there is a link to other information which allows to identify them – it should be seen as personal data within the meaning of the GDPR. Such is also supported by the ePrivacy Directive, which recognises the possibility of using cookies as a way of tracking the user online, and that their use should therefore be subject to the information obligations imposed by data protection law.[55]

Arguments for inclusion: no mention in the text – If metadata is indeed included within the notion of personal data as defined in the GDPR, it makes sense to deduce from this that it should also be included within the scope of the DCSD. After all, the definition of personal data refers back to the one in article 4(1) GDPR, without mentioning any exception for any kind of data. The fact that the wording of 'active' provision was removed from the final version of article 3(1) DCSD, also points towards an intention of the legislature to include the provision of metadata within the directive's purview. Indeed, if it wanted to make sure an exception for metadata was a part of the directive, the question has to be asked why it omitted it from its main text, to instead relegate it to the recitals, which – while often deemed instrumental for the purpose of interpretation, specifically by the Court of Justice – do not quite possess the same legally binding value that the main text has.

Arguments for inclusion: transparency and legal certainty – Indeed, as the European Data Protection Supervisor also pointed out in its opinion on the DCSD's proposal, the idea of creating a distinction of data based on whether it has been actively or passively provided by the

[53] European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users' 22
[54] Ibid 9
[55] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37, recitals 24-25

consumer, has no real support in data protection law.[56] The distinction is thus scarcely defined, and might therefore be hard to apply in practice. Presumably, where clicking on a post might be passive data provision, liking it might be active, but it is hard to know for sure. Moreover, splitting up the definitions of personal data, depending on if it is the GDPR or DCSD that is being applied, would be confusing from the consumer's point of view, especially seeing as such is not obvious from the definition the main provisions of the DCSD puts forward. The argument is to be made that, seeing as the consumer is defined in article 2(6) DCSD as someone who is acting in a non-professional capacity, the rules that apply to them should be clear and accessible, to ensure that they are aware of the scope of their rights, and can thus effectively enforce them. So a shared definition of personal data between the DCSD and GDPR should be preferred, for the benefit of transparency and legal certainty.

Arguments for inclusion: preventing abuse – As also mentioned by the European Data Protection Supervisor, the provision of metadata is less noticeable from the consumer's perspective, than that of other forms of personal data that they provide in a more active way. This means they will likely be less conscious of the scale of data gathering that the trader might be involved in, and thus be less hesitant towards it. In other words, the trader already has ample reason to prefer the collection of metadata over that of other kinds of data. Excluding metadata from the scope of the DCSD, would only give them more incentives to do so. We want to avoid a situation in which the trader will rely even more on metadata than it already does, just to be able to circumvent the application of the DCSD.[57] Encouraging traders to engage in less transparent forms of data collection, would be hard to reconcile with the importance both consumer and data protection law attach to ensuring the consumer is informed of what is going on.

Arguments for inclusion: economic value – As we already pointed out above, the collection of metadata will be an important part in the trader's efforts to create an identifiable profile of the consumer, which can be utilised for the purposes of targeted advertising. Simply put, it has at least as much economic value to the trader as more actively collected forms of personal data have. So going from the idea that the legislature included data provision contracts within the DCSD's scope in order to take account for certain business models, it makes no sense to then exclude an important component of such business models from the protection the directive offers.[58] Additionally, the consumer's interests are harmed in the same way, regardless of what kind of personal data is being collected. As metadata can be used so effectively to create a

[56] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 12
[57] Ibid
[58] Axel Metzger, Zohar Efroni, Lena Mischau and Jakob Metzger, 'Data-Related Aspects of the Digital Content Directive' [2018] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 90, 96

comprehensive profile of the consumer's identity, behaviours and characteristics, their privacy will be infringed on the same scale.[59]

Arguments for inclusion: recital 24 DCSD – Indications that point in favour of including metadata within the scope of application of the DCSD, can also be found in the recitals. As we already mentioned, recital 24 makes clear that the consumer does not necessarily have to perform their data provision obligations at the moment of conclusion of their contract with the trader. Instead, the provision can occur at a later time, i.e. during the consumer's enjoyment of the digital content or digital services in the contract. Besides user-generated content, metadata would be the main category of data which would be collected by the trader in this timeframe, so excluding it would in some way harm the effective application of this recital.[60]

Arguments for inclusion: the exception in recital 25 DCSD – Attention should also be paid to an exception article 25 DCSD makes to the exclusion of metadata that it stipulates. It provides that the provision of metadata will be included within the scope of the DCSD, where Member State law considers the situation to be that of a contract. However, for data provision to be covered by the DCSD, the existence of a contract, that is a valid under Member State law, will always be required. After all, article 3(1) DCSD clearly requires that there be a contract, and article 3(10) DCSD provides that the Member States' rules pertaining to the validity of such a contract should still apply to DCSD contracts. So a strict interpretation of recital 25 DCSD, would have as a result that it has overall no impact on how the directive's scope should be interpreted, and always allow for the inclusion of metadata. After all, as soon as the requirement that there exists a valid contract under national law, is met, this contract will fall under the exception to the exclusion of metadata in article 25 DCSD, and thus be included within the scope of the directive again.[61]

Arguments against inclusion: the Member States' autonomy – The main problem with unconditionally including metadata within the DCSD's ambit, is that it ignores the discretion the directive leaves to the Member States. Recital 25 DCSD makes clear that Member States, in transposing the DCSD into national law, enjoy the freedom to ignore the exclusion it provides, and extend protection to metadata providing consumers anyway. If however, the directive were to be interpreted in a way that metadata is in fact always included within its scope, such would mean that Member States are denied the choice whether or not to extend the directive's application, and thus are denied the option to still exclude it. So, not only would the

[59] Ibid
[60] Zohar Efroni, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' [2020] Common Market Law Review 799, 814
[61] Ibid

interpretation that metadata be included within the DCSD's scope, render this part of recital 25 DCSD meaningless, it would also infringe on the autonomy of the Member States, which the legislature clearly wanted to account for in this case.

Arguments against inclusion: no mention in the text – We mentioned that the directive's silence on the active or passive nature of the data provision, can be interpreted to be meant that the latter is included within its scope. In the same way however, can the lack of mention of metadata, be seen as a sign that it does not enjoy the directive's protection. For instance, looking at recital 24 DCSD again, when explaining how the consumer has the option to fulfil their personal data provision obligations only after the conclusion of the contract, it does not mention that such provision can be done through metadata. Instead, it only gives data that the consumer 'might upload or create' as examples, which points more in the direction of user-generated content, than that of cookies and IP-addresses.[62]

Exclusion of traders 'only' collecting metadata – The answer as to whether or not metadata is included within the DCSD's scope, seems to be nuanced in practice, however. It is easy to overlook that recital 25 DCSD does not necessarily exclude all collection of metadata from the DCSD's scope. Instead, it specifically targets traders who only collect this kind of data from the consumer. Therefore, the preferred interpretation seems to be that consumers who provide metadata, will enjoy the directive's protection, if they also provide other kinds of personal data. Of course, this solution is not optimal for the consumer, as it still incentives traders to focus on metadata collection to circumvent the DCSD's application. Furthermore, it gives the distinction between active and passive data provision – which once again, has no support in data protection law – a continued importance, a distinction which may be hard to apply in practice. However, it does technically mean that the definition of personal data in the DCSD, read on its own, remains consistent with the one in the GDPR. Moreover, it is well-suited to attain the likely purpose of drafting the exclusion in the first place. Article 2(1) DCSD defines the notion of 'digital content' very broadly: any data which the trader supplies to the consumer in digital form, is included. In practice, most online websites will use some sort of cookie system to collect information on their visitors – or at the very least keep track of their IP-addresses. So if all collection of metadata were to be covered by the DCSD, it would be applicable to any use of the internet. Presumably, every simple Google search, every consultation of Wikipedia, or a look at the menu on the website of your favourite restaurant, would enjoy the DCSD's protection, and thus theoretically, any malfunction of such a website could give rise to a legal claim. This clearly goes beyond the directive's intention to target certain business models. Recital 25 DCSD allows the scope of the DCSD to be narrowed, while still including the traders who are the most involved in the data

[62] Ibid, 814-815

gathering industry. The idea of narrowing the scope is also reflected in the fact that the recital also excludes situations is exposed to advertisements only to access digital content or digital services, without there being any conclusion of a contract involved.

Application of the exclusion – It should be wondered if the inclusion of recital 25 was truly necessary to achieve the narrowing of scope the legislature envisioned though. Presumably, in many cases, the economic value requirement we discussed earlier, could suffice on its own for this purpose. Moreover, this interpretation of recital 25 DCSD – that only the exclusive collection of metadata is excluded from the directive's scope – might mean that, in order to enjoy protection under the DCSD, the consumer needs to have an account – consisting of actively provided data – with the trader. However, regarding this last point, it should be noted that the metadata's use for identification of data subjects – and thus transforming other data into personal data –, should in our view be separated from its classification as personal data. So for instance, if a consumer uploads user-generated content – which is active data provision – to the trader's digital service, without having an account, but with an identifiable IP address, this data provision could still be covered by the DCSD. By rendering the uploader of the user-generated content identifiable, and thereby transforming this content into personal data meeting the GDPR's requirements, the at first excluded IP address will be gathered together with actively provided personal data, and thus also enjoy the DCSD's protection.

3. CONSENT IN THE DCSD

3.1. WHY CONSENT UNDER THE GDPR IS REQUIRED

Precedence of data protection law – When interpreting and applying the DCSD, the GDPR should always be kept in mind, and not just because the definition of personal data in article 2(8) DCSD, refers back to the one in article 4(1) GDPR. Article 3(8) DCSD provides that EU data protection law should be applied to the processing of the personal data provided by data paying consumers, as part of their contract with the trader under the DCSD. Specifically, it mentions that the provisions of the GDPR and ePrivacy Directive take precedence over those of the DCSD, in case a conflict between the two arises.

Processing of personal data in the GDPR and DCSD – The precedence of the GDPR will play an important role in practice, as an examination of the scopes of both instruments reveals that any personal data provision under article 3(1) DCSD, will most likely also amount to processing of personal data within the meaning of the GDPR. This makes sense, as once again, the definition of personal data of the DCSD refers back to the one in the GDPR. Of course, article 3(1) and recital 25 DCSD make exceptions for purely necessary data provision and exclusive metadata provision, respectively, but these only narrow down the DCSD's scope, without adding anything that would be outside of the GDPR's purview. Regarding the activity of 'processing' of personal data meanwhile, it must be noted that article 4(2) GDPR interprets this notion quite extensively. Any operation performed on personal data will be included, e.g. the collection, storage and use of it. When a consumer provides personal data to a trader under the DCSD, this will necessarily result in the trader collecting it, and by this very act, processing of personal data within the meaning of the GDPR will have taken place.

Overlapping personal scopes – Next, it should be mentioned that the personal scopes of the DCSD and GDPR seem to align quite well. Article 4(1) GDPR requires the person whose data is being processed, to be a natural person. Similarly, while it leaves room for the Member States to expand the scope of its application beyond consumers[63], article 3(1) DCSD makes clear that the directive will only apply to personal data provided by consumers, which article 2(6) DCSD defines as natural persons acting for non-professional purposes. The person to whom the consumer will provide the data is of course in principle the trader who grants them access to the digital content or digital services they desire. Article 2(5) DCSD defines the trader broadly, as any person acting for professional purposes. Meanwhile, the GDPR also allows any kind of

[63] DCSD, recitals 16-17

person, natural legal or otherwise, to be the data controller – defined in article 4(7) GDPR as any person in charge of determining the purposes and means of the processing of personal data – as well as the data processor – which is according to article 4(8) GPDR, any person who processes the data on the controller's behalf. While article 2(2)(c) GDPR also excludes any processing for non-professional purposes from its scope, this does not necessarily matter, because traders, as long as they are in charge of the personal data provided to them by the consumer, will be subject to the obligations imposed upon data controllers by the GDPR – or at the very least, if they collect the data on someone else's behalf, those imposed upon data processors.

Automated data processing – Lastly, when comparing the scopes of the DCSD and GDPR, it should be mentioned that the GDPR only applies to processing of personal data that is performed at least partly by automated means, or alternatively using some sort of filing system.[64] In this regard, the Court of Justice has stated that putting information on the internet is an act which is performed at least in part automatically.[65] Therefore, it can be concluded that whenever the consumer provides the trader their data using the internet, or even just using a computer of some kind, the GDPR's automation requirement is met. Of course, it is possible that the consumer provides their data with pen and paper. Even in that case though, it is more than likely that the data collection from then on will be automated, or at least systematically filed, for the trader to engage in large scale data analysis and profiling. It is therefore unlikely that this requirement will pose any practical problems for the application of the GDPR to contracts covered by the DCSD.

Lawful processing – The fact that virtually every data provision contract under the DCSD, is also covered by the GDPR, means that when collecting the data from consumers, the traders will always have to be mindful of their obligations under the GDPR, and the principles enshrined within it. One of the most important of these principles can be found in article 5(1)(a) GDPR, namely the idea that all data must be processed in a lawful manner. This entails that the trader – assuming they are the data controller here – must always have one of the legitimate grounds of article 6(1) GDPR underpinning the act of data gathering they are engaged in. Recital 38 DCSD confirms that any data provision under the directive, should be based on one of these grounds from the GDPR.

Legitimate grounds for processing – Most of the legitimate grounds enumerated in article 6(1) GDPR, will be of little practical use in the context of contracts covered by the DCSD. Most obviously, the justifications of article 6(1) GDPR – that the processing is necessary for the performance of the contract in question – and article 6(1)(c) GDPR – that it is needed in order to

[64] GDPR, art 2(1)
[65] Case C-345/17 *Buivids* [2019] EU:C:2019:122, para 38

comply with a legal obligation the controller is subject to – cannot be relied upon here. As we discussed above, article 3(1) DCSD explicitly excludes data provision solely for these purposes from its scope, so at least another ground will be needed in addition. The ground provided by article 6(1)(d) GDPR meanwhile, that processing is necessary for the protection of the vital interests of a natural person – that being the data subject themselves, or someone else entirely – will also be difficult to apply in practice. Recital 46 GDPR states that this ground is one of last resort, only to be relied upon when every other ground is 'manifestly' unavailable, and only if interests essential to someone's life are at stake. It seems unlikely that a lot of digital content and digital services – specifically those with a profit-based motive behind them – will meet this requirement, especially considering the fact that most healthcare services are excluded from the scope of the DCSD. Health applications that can be obtained without a prescription from a health professional, are still covered by the DCSD though[66], and might be the most likely kind of service the ground of article 6(1)(d) can be used for.

Processing for public interest reasons – When the trader in question is a government authority, a reliance on article 6(1)(e) GDPR might be opportune. This provision provides a legitimate ground for processing which the controller needs to engage in to perform a public interest task , or exercise its official authority. However, it should be noted that recital 27 DCSD provides that the directive does not apply to public services, or at least when the digital means are only used to transmit the service to the consumer, thereby severely limiting the practical application of article 6(1)(e) GDPR in the context of the DCSD.

Processing for the purposes of the controller's legitimate interests – One ground for processing the European Data Protection Supervisor paid particular attention to in its opinion on the DCSD's proposal, is that of processing necessary for the legitimate interests of the controller or a third party, contained in article 6(1)(f) GDPR.[67] As we pointed out above, the legislature included data provision contracts within the scope of the DCSD, to take into account business models in which the personal data is collected in order to extract economic value from it, specifically by using it for the purpose of targeted advertising. In other words, such targeted advertising will be the main legitimate interest pursued by data gathering traders in the context of the DCSD. In this regard, Recital 47 GDPR recognises direct marketing purposes as a legitimate interest that could meet the requirements of article 6(1)(f) GDPR. However, it should be noted that article 6(1)(f) GDPR provides that the legitimate interests relied upon, could be overridden by the interests of the data subject – e.g. their fundamental rights. As explained by

[66] DCSD, recital 29

[67] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 17

the Article 29 Working Party, invocation of this ground requires the execution of a balancing test. Only when a proper balance has been achieved between the interests of trader and data subject, can the former be relied upon for the purposes of lawful data processing.[68] The European Data Protection Supervisor seems however sceptical that such a balance is possible in the context of targeted advertising following data provision under the DCSD. In this regard, it points at what the Court of Justice decided in *Google Spain*[69], regarding a data subject who wanted certain search results removed from Google searches using their name. The Court of Justice concluded that the economic interests of the trader in providing complete information – and thus a comprehensive service – to its users, could as a rule not outweigh the data subject's right to privacy and personal data protection.[70] Specifically concerning targeted advertising, the Article 29 Working Party recommends a similarly privacy-minded approach. It concedes that data controllers might have a legitimate interest in discovering the preferences consumers might have, for instance to allow them to make more personalised offers. However, if, in order to allow targeting, the trader engages in extensive online monitoring of the consumer, as well as in the creation of detailed profiles of their behaviours, characteristics and preferences, such would likely significantly invade the consumer's privacy. Therefore, when involved in a business model of large scale online profiling for targeted advertising purposes, traders can most likely not rely on their legitimate interests in applying such a business model to justify the data processing they occupy themselves with. The privacy of the consumers will be impacted too significantly, to not require their consent to the processing.[71]

Processing based on consent – The conclusion seems to be that in most cases, the trader – especially the one who wants to use the provided data for targeted advertising purposes – will have little choice but to rely on the last legitimate ground left, namely that of article 6(1)(a) GDPR, the consent of the consumer to the data processing. This means the trader will also have to comply with the plethora of requirements the GPDR imposes, in order for this consent to be able to lead to lawful data processing. However, even if another legitimate ground for processing can be found, the argument is to be made that the GDPR's conditions for consent should be met for any contract that is covered by the DCSD. On a conceptual level, it seems indeed hard to imagine how a consumer can freely and validly consent to the provision of their personal data – as defined in the GDPR –, and thus conclude a contract covered by the DCSD, without also meeting the GDPR's requirements– which serve to ensure that this consent is sufficiently freely

[68] 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' WP 217 25-26
[69] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 17
[70] Case C-131/12 *Google Spain and Google* [2014] EU:C:2014:317, para 99
[71] 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' WP 217 25-26

given. In this regard, the precedence the GDPR has over the DCSD, as stipulated in article 3(8) DCSD, should be mentioned again, as well as our conclusion above that the GDPR is applicable to any data provision contract which enjoys the DCSD's protection. Indeed, a contract will only be validly concluded, if the parties have consented to its obligations. If one of the main obligations of the contract is the provision of personal data, than that means that consent to data provision is required, and that all conditions the law – both national and European – puts on such consent, should be complied with. This idea is also supported by the European Data Protection Supervisor, who stresses that the GDPR is applicable in horizontal situations – such as relations between contractual parties – and that therefore, whether this consent was freely given, should be assessed with its provisions in mind.[72] Additionally, the idea of a requirement of valid consent is also implied in recital 24 DCSD. When explaining how the data provision in question can also occur after the conclusion of the contract, the recital mentions that such could happen at the moment the consumer gives consent to the trader to process the personal data, which might be enveloped in the user-generated content uploads.

3.2. FREELY GIVEN CONSENT TO A CONTRACT UNDER THE GDPR

Freely given consent in a contractual context – Recital 38 DCSD reaffirms that the requirements the GDPR imposes on consent must be complied with, if such consent is the legitimate ground applicable to data provision under the directive. A look at the definition of article 4(11) GDPR reveals a list of conditions the consent must meet, one of which being that it should be 'freely given.' In this regard, article 7(4) GDPR adds that it must be taken into 'utmost account' that the data subject has concluded a contract, the performance of which is dependent on their consent to processing of personal data. Recital 43 GDPR goes further, and states that when performance is dependent on such consent, without this consent actually being necessary for the performance, it must be presumed that the data subject cannot give free consent within the meaning of the GDPR. This requirements clashes directly with the whole concept of the data paying consumer under the GDPR. Indeed, the performance of a contract covered by the DCSD will be dependent on the consumer's consent to data provision. After all, if they does not consent, there is no lawful data provision, and no counter-performance which puts the situation within the purview of article 3(1) DCSD. Furthermore, data provision is not allowed to be necessary for the performance of the contract, as that would mean it is covered by one of the necessity exceptions, and thus excluded from the directive's scope.

[72] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 17

A rebuttable presumption – Simply put, a strict interpretation of article 7(4) GDPR, would entail that no data provision under the DCSD, could ever amount to lawful processing allowed under the GDPR. However, the fact is that the same legislature who drafted the GDPR, also enacted the DCSD. As the legislature clearly wanted data provision as a counter-performance to be legal, this means that an interpretation of the GDPR must be possible, which allows such to occur.[73] Indeed, recital 43 GDPR only provides a presumption that consent is not freely given. The European Data Protection Supervisor believes that rebuttal of this presumption should be possible in the context of the DCSD. It states that the free character of the consent should always be assessed on a case by case basis, taking into account the transparency of the processing, as well as the balance of power between the parties to the contract. Therefore, a data provision contract under the DCSD will be lawful under the GDPR if these other conditions are complied with.[74]

Information requirements – As the European Data Protection Supervisor states, how transparent the processing is, will depend on what information the trader has provided the consumer.[75] Indeed, consent needs to be 'informed', in order to meet the requirements of article 4(11) GDPR. The consumer will only be able to give free consent, if they know what it exactly is that they are consenting to. As the Article 29 Working Party puts it, there can be no risk of deception.[76] First of all, this means that the consumer in question needs to be informed as to what purposes the trader will process the data for, after the consumer has provided it to him.[77] As consent under article 4(11) GDPR also needs to be 'specific', the consumer should be given the opportunity to consent to every purpose separately.[78] This means that the trader will have to enumerate every use they might have for the data – e.g. profiling, improvement of service etc. – to the consumer.[79] In addition, it must be ensured that the consumer knows that they are consenting to data processing. The information provided should be accessible, and use clear and plain language.[80] The request to consent to data provision should stand out from other requests and information the trader might simultaneously supply them with.[81] For children under sixteen years old, consent from a parent shall be required.[82] In addition, all requirements national civil

[73] Axel Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' [2017] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 2, 5
[74] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 17
[75] Ibid, 16
[76] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' WP 187 12
[77] GDPR, recital 42 and arts 13(1)-(2)
[78] GDPR, recital 43
[79] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 14 and 16
[80] GDPR, recitals 32 and 42, arts 7(2) and 12(1)
[81] Ibid
[82] GDPR, art 8(1)

law imposes as regards the legal capacity to consent to a contract, should apply to consent to data processing under the GDPR.[83] Lastly, as article 4(11) GDPR requires, the consent should also be 'unambiguous', and be given through a 'statement or a clear affirmative action.' A deliberate and conscious act of consent will be required. For instance, the fact that the consumer did not untick a pre-ticked checkbox stating consent, should not be enough for consent to be unambiguous, and thus informed.[84]

A genuine choice – The second factor which should be taken into account when assessing whether consent to the data provision contract is freely given within the meaning of the GDPR, relates to the position the contractual parties have, in relation to one another. Recital 43 GDPR states that there can be no freely given consent to data processing, when there is a clear imbalance between the data subject and the controller. The European Data Protection Supervisor emphasises that such an imbalance might result from an information asymmetry between the parties[85], which ultimately brings us back to the information requirements above. However, as recital 42 DCSD clarifies, consent will also not be free, if there is no 'genuine choice' available to the consumer. This freedom to choose can be interpreted in three ways. First of all, it must be examined if the consumer can choose to contract with other supplier for the provision of equivalent digital content or digital services, instead of with the trader concerned. This will require an analysis of the market position of the trader in question, in comparison to other competing traders.[86] Indeed, if the trader in question has a dominant position on the market, or the market is very concentrated, the consumer might be robbed of any free choice at all.[87] However, the free character of consent should not be made dependent on the state of the market alone. Data controllers should not have to keep track of market developments, in order to know if they are complying with the GDPR's requirements.[88] Therefore, the second way in which there must be a genuine choice for the consumer, relates back to the payment options the trader gives him. Simply put, the consumer can only freely consent to data provision, if they have the option to access the digital content or digital service in question, without having to provide their personal data.[89] In other words, the trader might be obligated to offer a version of the digital content or digital service they supply, that does not rely on data provision, i.e. requires a

[83] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on Data Protection Law* (Publications Office of the European Union 2018) 112
[84] GDPR, recital 32
[85] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 16
[86] Ibid
[87] European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (March 2014)' 35
[88] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' 11-12
[89] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content'16-17

payment of a monetary price instead.[90] The final way in which the consumer must have free choice, relates to the consequences that not granting consent might have for him. Recital 42 GDPR states that a data subject will not be able to freely consent to data processing, when they are unable to refuse their consent, without it negatively affecting him. The negative effect might come from the fact that the digital content or digital service in question, is absolutely essential for them to be able to live their normal life[91]. In addition, if the quality or performance of the digital content or digital service might be significantly downgraded by the trader, because the consumer refused their consent to data processing, such might also result in a finding that the consumer is unable to give free consent in this case.[92]

3.3. A SEPARATE DEFINITION OF CONSENT FOR THE DCSD

Fighting the information-asymmetry – The information requirements it imposes on the consent of data subject, reveal one of the underlying objectives that the GDPR seems to have: fighting the information-asymmetry between the data subject and the data controller. Seeing as data gathering can occur through indirect means such as through profiling and the use of metadata, it can be difficult for a data subject to know whether their data is being processed in the first place, let alone what the scope and purpose of it is. Without proper enforcement and monitoring of the rules provided by the GDPR, it is easy for the controller to deceive the data subject in this regard.

Preventing misinformation in the DCSD – This idea of wanting to protect the weaker party in a data provision transaction, and then specifically against deception and misinformation, can also be found in the DCSD. Article 7 DCSD's subjective conformity requirements require the digital content or digital services concerned to be in accordance with wat has been explicitly agreed between the trader and the consumer, either in the contract itself, or in a verbal agreement of some kind. The directive's requirements could have stopped here, in which case the trader only has to provide what they have directly promised, to be compliant with their obligations under the DCSD. Instead, the legislature chose to include the objective conformity requirements of article 8 as well, which serve to take into account the reasonable expectations the consumer might have as regards the provided digital content and digital services, beyond what is stipulated in the contract at hand. Some of the requirements concern expectations the

[90] Paul Voigt and Axel vom dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017) 96
[91] Axel Metzger, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' [2017] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 2, 5
[92] European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679' 13

consumer might reasonably have based on the nature of the content or service[93] or its normal purpose.[94] More relevant here though, are the requirements that account for the consumer's reasonable expectations that are based on impressions created by the trader – or other parties in the chain of transactions leading up to the supply of the digital content or digital service to the consumer –, e.g. through advertising or labelling.[95] If the trader misrepresents certain aspects of the digital content or digital service concerned – or makes no efforts to remedy misrepresentations made by previous links in the chain of transaction – this could lead to application of the remedies the DCSD provides the consumer with. So while it does not directly concern the data provision aspect of the contract, the DCSD clearly upholds the same goal of preventing misinformation of the consumer, that the GDPR bolsters.

Violations of the GDPR should not be rewarded – Article 4(11) GDPR affirms that the notion of 'consent' in principle comes down to an agreement on the consumer's part to the processing of their personal data. However, as we discussed above, many conditions are added – e.g. that it is free and informed – to this agreement, in order for it to qualify as valid and thus be used as a legitimate ground for data processing. These requirements should arguably be met for any contract covered by the DCSD, otherwise the trader would be in violation of the GDPR, which means the contract itself might not be valid. However, an infraction of the GDPR in this way should not prevent the DCSD from being applicable. After all, both the conditions for consent in the GDPR and the requirements and remedies of the DCSD are meant to protect the weaker party in the transaction, specifically against misinformation. The situation should be avoided in which a consumer-data subject is not properly informed – in accordance with the standards of the GDPR – by the trader-controller, and that this lack of awareness then results in the contract being outside the scope of the DCSD, and them being denied the protection against misinformation it offers. Simply put, a data paying consumer should not have to been made aware of their status as such, in order for them to rely on the remedies provided by the DCSD.. Someone whose data has been obtained without proper consent, should still be entitled to properly functioning digital content and digital services. They should not be punished for their ignorance, as such would be contrary to the objective of to prevent misinformation of the consumer, upheld by both the DCSD and the GDPR. In the same vein, traders should not be incentivised to ignore their information obligations under the GDPR, by allowing them to avoid responsibility under the DCSD as a reward for doing so. Similarly, when there is a clear imbalance between the positions of the trader and consumer, which prevents the consumer to give free consent to the standards upheld by the GDPR, such should also not prevent the

[93] DCSD, art 8(1)(b) and (c)
[94] DCSD, art 8(1)(a)
[95] DCSD, art 8(1)(b) and (d)

consumer from relying on the DCSD. After all, the weaker the consumer's position is, the more imperative it will be for them to be able to properly enforce the conformity requirements the directive puts forward.

An act of data provision should suffice – So for a situation to be within the scope of the DCSD – or at least for the consumer to be able to rely on it – it should not be required that it be proven that all the conditions for consent under the GDPR are met. The validity of the consent under the GDPR should not affect the validity of the trader's obligations under the DCSD.[96] In order to ensure that both the GDPR and DCSD are respected as to their objective of protecting the weaker party in the transaction against misinformation, it should simply suffice that it be proven that personal data has been provided by the consumer, for the DCSD to be applicable. The very act of data provision, even unknowingly, through use of the digital content or digital service, could then be seen as an implicit agreement by the consumer to a contract covered by the DCSD.

3.4. THE BURDEN OF PROOF FOR CONSENT

The consumer's burden in the DCSD – Even if the DCSD imposes no real requirements for consent, other than an – at least implicit – agreement to data provision, such an agreement still needs to be proven, in order for the directive to be applied. It will need to be shown that an act of data provision within the meaning of article 3(1) DCSD has taken place – or the consumer has at least undertaken to do so – for the contract to be within the DCSD's ambit. As the consumer will typically be the claimant in any case enforcing the directive, it would makes sense that they would be the one who would have to prove that the situation is within the scope of the DCSD in the first place. Indeed, recital 59 DCSD states that in principle, it will be for the consumer to prove that there is a lack of conformity in the supply of the digital content or digital services concerned, which could justify an invocation of its remedies. Simply put, if the consumer has the burden of proof regarding a violation of the DCSD's requirements, this might mean that they also have this burden when it comes to proving its applicability.

Data provision is hard to prove for the consumer – If the consumer is indeed the one that should prove that personal data has been provided – and thereby consent has been given to a contract covered by the DCSD – it should be wondered how they would go about accomplishing this. If they have an account with the digital content or digital service that they claim is subject to a lack of conformity, then presumably they can just point out the existence of such an account, to

[96] Axel Metzger, 'A Market Model for Personal Data: State of Play Under the New Directive on Digital Content and Digital Services' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V* (Bloomsbury 2020) 6 <https://ssrn.com/abstract=3666805> accessed on 29 April 2023

prove that an agreement to data provision has been made. After all, their account information will usually include enough personal data to meet the directive's requirements, and will also be of the kind that enables their identification, and thus a linkage to the data. The situation will be different however, if the consumer has no account with the trader, or one using a name and email address that cannot be traced back to him. In this case, the trader will still be able to gather personal data of the consumer. Their preferences and characteristics – economically valuable data relating to them – can still be determined through examination of the user-generated content they upload and through behavioural tracking. As we discussed, the trader can then identify the consumer, despite not having an account, by combining all this non-identifying data in order to single out a profile with unique traits. Alternatively, they can rely identifying metadata, such as IP addresses and identifying cookies, to enable the consumer's identification. When the trader employs these techniques, such will result in an act of personal data provision which allows the DCSD to be rendered applicable. However, in practice, it can be difficult to know, and even harder to prove, for the consumer what personal data of theirs has been gathered. They would need to have an overview of the profile the trader has been assembling of him, information they can only get from the trader themselves. The trader has all the information here, and nothing stops them from hiding it from the consumer. Even if the consumer has an account, the trader has the power to delete it if it senses a legal claim might be coming its way, thereby rendering the consumer without proof of data provision, and thus without effective access to the remedies of the DCSD. Once again, the trader is incentivised to violate their information obligations under the GDPR. After all, if the consumer does not know to what extent their data is being processed, they can also not prove it in court. The shared goal of the DCSD and GDPR of preventing misinformation and deception of the consumer, would be counteracted, if it were the consumer who had to bear the burden of proof under the DCSD that personal data has been provided. In addition, any imbalance in the positions of the parties, which prevents the consumer from giving free consent meeting the requirements of the GDPR, would be aggravated, if the trader were given the power to deny the consumer proof of their data provision, and thereby access to ways to enforce their contractual rights.

Application of the GDPR's evidentiary rules – The conclusion to be drawn, is that it should be the trader, not the consumer, who should bear the burden of proof as regards whether or not data provision under the DCSD has taken place. After all, taking into to the weaker position of the consumer, this is necessary to ensure that the DCSD can be effectively applied. Such a reversal of the burden is also supported by article 7(1) GDPR, which provides that it is the data controller who should prove that the conditions of consent the GDPR imposes, are complied with. So when a data subject claims they have not given consent that meets the requirements of the GDPR, it will be for the data controller to disprove this. The fact that the GDPR and the DCSD

employ two separate definitions of consent, does not mean that article 7(1) GDPR is irrelevant here. In defining consent, article 4(11) GDPR still has the idea of an agreement to data processing at its core. So the definition of consent under the DCSD is contained within the one supplied by the GDPR, which simply imposes additional requirements on it. Therefore, the rules article 7(1) GDPR provides as regards the burden of proof for consent, could also be applied in the context of the DCSD.

The best placed party should disprove consent – It should be noted however, that article 7(1) GDPR should not be applied strictly in order to ascertain who bears the burden of proof for consent under the DCSD. In the GDPR, proving the presence of valid consent is not about determining whether the regulation is applicable in general. Instead, it is about the substantial obligations it imposes, and whether the data controller has violated those. Therefore, it will be the controller who will be the one who wants to prove that the conditions for consent have to be complied with. Under the DCSD, the reverse is true. Here, proving the existence of consent concerns the applicability of the directive, and therefore the possibility to invoke the remedies it provides for consumers. This means that the trader will want to instead prove that there was no consent, so they can avoid application of and thus responsibility under the directive. Article 7(1) GDPR, and its notion that the data controller must 'prove consent', must also be interpreted inversely. Under the DCSD, they will instead have the burden to prove that there was no consent, as soon as the consumer claims that there in fact was. Presumably, the legislature included the evidentiary rule of article 7(1) GDPR, in order to ensure that the controller can be effectively held accountable for their violations, as they are the one who is the 'best placed' to provide evidence as to whether or not the imposed consent requirements have been met.[97] After all, the practical difficulties consumers have in proving valid data provision under the DCSD, will also be in play for data subjects trying to disprove such under the GDPR. In order to uphold this idea that the party best placed to do so, should bear the burden of proof, article 7(1) GDPR should be applied in the context of the DCSD, in a way which imposes on the trader the burden to disprove any claims of valid consent put forward by the consumer.

The best placed party principle in the DCSD – So the idea that the best placed party, i.e. the trader, should be the one who provides evidence pertaining to consent under the DCSD, is prompted by practical considerations as regards the effectiveness of the protection it provides to consumers, on the one hand, and by application of the GDPR on the other. However, support can also be found in some off the rules relating to burden of proof for lack of conformity, found

[97] Brendan Van Alsenoy, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' [2016]] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 271, 283

in the DCSD itself. Article 12(2) and 12(3) DCSD provide that while proving the lack of conformity itself is still for the consumer, under certain conditions, it is for the trader to then disprove that this lack of conformity was present at the time of supply – or during the period of supply. Similarly, article 12(4) DCSD gives the trader the burden to prove that the lack of conformity is caused by the digital environment of the consumer, instead of making the consumer prove that such is not possible. Recital 59 DCSD clarifies that both these provisions are founded on the idea that the trader will have an easier time discovering why there is a lack of conformity in the case at hand, than the consumer will. As the recital explains, due to their superior technical knowledge of their own product, they are namely the best placed to provide evidence in this regard.

A duty of cooperation – Another rule that is inspired by the idea that the best placed party to do so, should be the one providing the evidence, can be found in article 12(5) DCSD. This provision introduces the idea that the consumer has a duty to cooperate with the trader, and support them in their efforts to prove that the lack of conformity is due to the consumer's digital environment. The directive adds that if the consumer refuses to cooperate, the penalty will be another reversal of the burden, which means it will then be them who have to prove that the lack of conformity is not due to their digital environment. Recital 60 DCSD adds that this duty entails that the consumer should provide the trader with all information they possess, and might even have to allow them to access their digital environment for themselves. Perhaps, even if all of the above is to be ignored, and the burden for proving consent under the DCSD, is still with the consumer, this idea of a duty of cooperation can be applied analogously. Indeed, the GDPR seems to impose upon the trader such a duty when it comes to proving that data provision has taken place. Article 15(1) GPDR gives data subjects the right to know whether their personal data is being processed by the controller, as well as a right to access it. In addition, article 15(3) DCSD allows them to ask for a copy of the processed data. So even if the burden of proof as to whether data has been provided under the DCSD, remains with the consumer, as a data subject, they can invoke article 15 GDPR to make the trader provide their proof for him. While not a reversal of the burden of proof on paper, the implications will presumably be the same.

4. CONCLUSION

The notion of 'provision of personal data' in the DCSD – A combined analysis of the requirements of the DCSD on the one hand, and the definition of personal data in the GDPR on the other, has provided us an exhaustive list of conditions that a consumer should comply with, in order to be engaged in an act of personal data provision which leads to protection under the DCSD.

First of all, they must be rendered identifiable, either by the personal data provided – or an amalgamation of it – itself, or because this data is somehow linked to other data, which does identify him. Account information provided by the consumer, directly identifying metadata, or profiling done through an extensive combination of behavioural data, can all be used to this effect.

Secondly, the data must 'relate' to them in some way as a natural person, that is, reveal something about their identity, characteristics, preferences or behaviours, or alternatively be able to be used to evaluate them or influence their position. Virtually all content the consumer uploads or shares using the digital content or digital service in question, will qualify as such, even when it does not directly concern him.

Thirdly, the data provided must have some sort of value to the trader they provide it to, that goes beyond what is necessary for the trader to comply with legal obligations they are subject to, or what is needed for them to effectively provide the digital content or digital service in question. Most commonly this additional value will be of an economic nature, extracted through the use of the data for the purpose of targeted advertising. The value the data may have to the consumer is of little importance here however, it is the trader's perspective that counts.

Fourthly, the provision of data in question, may not happen simultaneously be a provision of something of direct monetary value – a payment in a conventional or digital currency. When such a mixed payment occurs, the consumer should be primarily seen as a price paying consumer. Of course, the data they have provided, will still enjoy the protection provided by the GDPR. If the provision is not simultaneous and intertwined, but instead separate and used for different aspects of the digital content or digital services, the consumer may still be classified as a data paying consumer, for the aspects covered by their data provision. However, as soon as the conformity of the parts they paid a price for are affected, this payment in price takes precedence.

Finally, the data provision in question may not solely consist of metadata. In this regard, the notion of metadata encompasses both data which can be used to identify the consumer's device,

and thereby themselves, as well as any personal data obtained through tracking their online activities. It should be noted that, even when not covered by the DCSD, this metadata can still be used to link an identifiable consumer to other kinds of data. It thereby transforms this data into personal data, which means the data provided goes beyond metadata, and thus allows this metadata to be covered after all.

No conditions for consent – Barring those relating to their own identity as a consumer or to that of the trader, no other conditions should be complied with, in order for a provision of personal data to be within the scope of the DCSD. The requirements of the GDPR should still be complied with for any provision of personal data of course. Specifically, the provision must be based on a legitimate ground, which usually means it will have to meet the extensive requirements for consent the regulation puts forward. The GDPR's conditions for consent have a significant impact on the trader: they mean they have to comply with certain information obligations, and might compel them to give the consumer another option to enjoy the digital content or digital services they offers, which does not involve the provision of their personal data. While, however, these requirements of the GDPR must be complied with for the data provision to be legal, they are not necessary for the DCSD to be applied. The mere fact of provision of personal data to the consumer – even unknowingly, through use of the digital content or digital service – should be seen as an implicit agreement to the data provision contract, which suffices for the consumer to invoke the protection the directive grants them. After all, imposing the GDPR's requirements here, would incentivise the trader to violate them, and would undermine the effective application of the DCSD. For these same reasons, the burden of proof as to the provision of personal data should be on the trader. Seeing as they will have a better overview of the data provision that has occurred, than the consumer, they are in the best place to do so. For the DCSD to be applied, the consumer should simply claim they have provided personal data within the meaning of article 3(1) DCSD. The trader can then avoid application of the directive, by proving that one of the aforementioned conditions for provision of personal data has not been fulfilled.

Impact of the GDPR on the DCSD – It is clear that the provisions of the GDPR have a significant impact on how article 3(1) DCSD should be interpreted. Most obviously, the definition of personal data – and thereby its requirements of identifiability and relatedness – provided by the GDPR, is also to be applied in a DCSD context. The wide interpretation of the notion of personal data put forward by the GDPR – any data 'about an identifiable natural person suffices – results in an equally extensive scope of application for the GDPR. Other concepts which have been developed in the context of data protection law, such as identifiability through the use of metadata, profiling through behavioural data, and economic value through targeted advertising,

have also proved useful in applying the DCSD. Moreover, the necessity exceptions in article 3(1) DCSD are clearly inspired by – and should thus be interpreted in the same way as – the legitimate grounds for processing in article 6(1)(b) an 6(1)(c) GDPR. Similarly, the notion of metadata – relevant as the exclusive collection of it does not lead to the DCSD's protection – must be filled in by referring to data protection law, in absence of a clear definition in the directive itself. More directly, the GPDR looms large over the DCSD, as any provision of data under the latter, must comply with the requirements of the former. After all, any data provision under the DCSD, will also be covered by the GDPR, which means a consumer under the DCSD, will also enjoy protection as a data subject under the GDPR. Indeed, it is the stringent requirements by the GDPR, relating to information obligations and the balanced position of the contractual parties, which might steer away the trader from offering contracts requiring data provision from the consumer, or might at the very least motivate them to offer alternatives. In addition, because of concerns that the trader might want to violate these requirements in the GDPR, in order to avoid application of the DCSD, the definition of consent under the DCSD will be very permissive. These same concerns, together with an application of article 7(1) GDPR, have also helped us in outlining the principle that the best placed party should provide evidence for consent. In the same vein, the data subject's rights under the GDPR, might result in a duty of cooperation for proving consent under the DCSD. The GDPR has therefore also had an influence on the burden of proof rules that apply under the DCSD. This interplay between the two is wat makes the notion of the data paying consumer in article 3(1) DCSD is so interesting: how the rights and requirements of data protection law are interpreted, might unwittingly also affect how those of an instrument of consumer law are to be applied.

Similar principles, different scope – The GDPR and DCSD hold up the same fundamental idea: the weaker party in a situation of data provision, should be protected against the stronger party in the transaction. While both instruments recognise that any sort of abuse of an imbalance of power should be combated, they are particularly concerned with the imbalance that might result from the information-asymmetry between the parties. Both the requirements for consent in the GDPR, and those for conformity in the DCDD, serve to discourage the more powerful party from deceiving or misinforming the weaker party as to the nature and consequences of their transaction. With all this in mind, it would be easy to assume that their scope of application, at least pertaining to the here discussed notions of 'consent' and 'personal data', would also be similar. As discussed, article 3(8) DCSD indeed provides that the GPDR's requirements – which includes those for consent – are indeed applicable to data provision under the DCSD. Similarly, the definition of personal data in article 2(8) DCSD refers back to the one in article 4(1) GDPR. However, while the rules of the burden of proof should still be the same, the notion of 'consent', required to apply the DCSD, is separate and less stringent than the one in the GDPR, due to the

different role – defining scope versus substantial obligation – the concept serves in both instruments. Likewise, the DCSD has a different, narrower view of what personal data provision should be included within its scope, than the GDPR does. While the exclusion of sole provision of metadata and the priority of payments in price, that the DCSD adds, are interesting, the true nature of the directive becomes clear from the necessity exceptions in article 3(1) DCSD, and the requirement of additional – usually economic – value it implies. The big divide between the GDPR and the DCSD is revealed here. The former is inspired by general human rights concerns, relating to the privacy of the citizens of the Union. The latter meanwhile, is a part of the body of consumer law, which traditionally concerns economic transactions. The main concern of the DCSD is that the consumer be treated fairly, that they get the value for money they expect and deserves. This in turn is at least partially linked to considerations originating from competition law, relating to the possible abuse of market power by the trader, and the objective of ensuring a level playing field in the Member States. The option of data provision seems indeed tacked on to the more traditional payment in price, an thus wants to stay in line with the economic interests it represents. This not only explains why the economic value requirements is included at all, but also why the value is to be appreciated only from the trader's point of view. The value the consumer allocates to – the infringement of – their privacy is of little importance when determining the scope of the DCSD. Despite the fact that it does not matter to the consumer – their privacy has been derogated from anyhow – the purpose the trader has for the data is of primary importance. Specifically it will be relevant that they can make a profit off of the personal data provided, which can be seen as a replacement for the value of the money they would have gotten from a price paying consumer. Where the GDPR serves to ensure that the personal data of the data subject is duly protected, the DCSD wants to prevent that the trader profits off of the provision of such data, without providing at least an adequate product in return. This less ambitious attitude is reflected in the more restrictive conditions the DCSD provides for the notion of personal data provision, and thus for the scope of its application.

Incongruences lead to a lack of legal certainty – Applying the DCSD and the GDPR together can lead to some apparent incongruences, which need to be reconciled. Most obvious is the juxtaposition between the scepticism article 7(4) and recital 42 GDPR exhibit towards data provision in the context of contractual obligations – and the free character of the consent to it, specifically, and the fact that such contractual provision of personal data, is exactly what article 3(1) DCSD envisions. Then there is the fact that equating the notion of consent under the DCSD to the one outlined in the GDPR, would create a situation where provisions that serve to protect the consumer in one way, would rob them of protection in other ways. So despite the fact that the GPDR's principles explicitly apply to data provision under the DCSD, and that it has a definition for consent to such data provision, such should not be used to decide whether a

contract is covered by the DCSD. Lastly, there is the exclusion of sole provision of metadata under the DCSD, which has no support in the GDPR, as well as the burden of proof rule of article 7(1) GDPR, which should be applied inversely in the context of proving the applicability of the DCSD. It is indeed to be wondered why the DCSD did not provide a definition of consent, or clarified what role the requirements put forward by the GDPR – specifically those in article 7(4) GDPR – should play in its application. Similarly, it is to be argued that the legislature should have made more of an effort to describe what should count as data provision under the DCSD – beyond just referring to the GDPR's definition –, as well as to how the burden of proof regarding it should be divided. Furthermore, that the exclusion of the sole provision of metadata has been relegated to an – ambiguously worded at that – recital is unacceptable. The scope of application of a directive should be made clear in its main provisions. In this contribution, we have tried to fill in the gaps the legislature left, in a way which would ensure the effectiveness of the protection the DCSD envisions. However, our conclusions here are not set in stone, and may be dismissed by the Court of Justice at any moment. Consumer law should be transparent and clear, so a consumer – who is after all, not acting in a professional capacity – should be able to easily know what the scope of their rights are, so they can effectively enforce them. Instead, an examination of the scope of application of the DCSD, as regards data paying consumers, brings one into a legal minefield of overlapping, contradicting and absent rules. Omissions by the legislature, in particular as to the interaction between the DCSD and the GDPR, have left the data providing consumer with a lack of legal certainty, as to under what conditions they can enjoy the DCSD's protection. This is rather poignant, as recital 3 DCSD cites increasing such legal certainty, as one of the main motivations the legislature had for adopting the harmonised rules of the DCSD in the first place.

The arbitrariness and ineffectiveness of the DCSD for data providing consumers – The conclusion of this contribution seems to be that the inclusion of data paying consumers within the scope of the DCSD was not well thought out by the legislature, or at least executed poorly. Even if the scope of application were more clearly defined in this regard, however, it is doubtful that data providing consumers could effectively enforce their rights under the DCSD, or at least as effectively as those paying a monetary price. After all, the whole system of remedies of the directive, seems built on the idea that, if all else fails, the consumer can at least end the contract and get their money back, pursuant to article 16(1) DCSD This option is not available for data paying consumers. Even if the personal data is returned, the data processing cannot be undone, nor can an infraction of someone's privacy. Barring this threat of restitution, it is to be wondered how consumer can effectuate compliance from the trader, without relying on remedies that go beyond what is provided in the directive. Lastly, the requirements the DCSD does provide for an act of data provision to be included within it scope, are too restrictive. If the provision of

personal data is indeed to be principally seen as an alternative to a monetary payment, then the economic value the data has for the trader, should be decisive. In that case, it does not make sense why it is only provision of 'personal' data, as defined in the GDPR, that enjoys the directive's protection. Surely, following the economic logic of consumer law, any provision of data – personal or not – that allows the trader to profit off of it, should be included. Conversely, if article 3(1) DCSD is based on the idea that the consumer should have a right to properly working digital content and digital services, because they have sacrificed their valuable personal data – and thus some of their privacy – for it, then it should be asked why the economic value requirement still exists. Surely, the consumer should not care what purpose the trader has for their data, their privacy will be harmed all the same. Simply put, the cumulative application of the conditions the DCSD puts to its application, leads to an unjustified, and thus arbitrary exclusion of some categories of consumers from its protection. Alternative applicability of these conditions could be a suitable solution. This would mean that data provision would enjoy the DCSD's protection, when it has either privacy-related value to the consumer, or economic value to the trader. Perhaps though, as the European Data Protection Supervisor has suggested in its opinion on the DCSD, we should go further, and abolish both requirements. In other words, any act of supply of digital content or digital services would be included within the DCSD's scope, regardless of what – if anything – the consumer provided in return.[98] Indeed, in a digital economy, the protection of consumers should not be limited by their classification as economic actors. An overly extensive application of the DCSD could then be remedied by defining the – currently very broadly and vaguely described notion of digital content, more restrictively. We can only hope that future revisions of the DCSD by the legislature, will take these considerations into account. As things stand now though, the notion of the data paying consumer in article 3(1) DCSD, is a poorly, unfairly and ineffectively defined one, and will remain so for the foreseeable future.

[98] European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content' 10-11

BIBLIOGRAPHY

EU LEGISLATION

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) [2016] OJ L119/1

Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L171/12

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37

Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1

Directive 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28

CASE LAW

Case 352/85 *Bond van Adverteerders v State of the Netherlands* [1988] EU:C:1988:196

Case C-70/10 *Scarlet Extended* [2011] EU:C:2011:771

Case C-131/12 *Google Spain and Google* [2014] EU:C:2014:317

Case C-582/14 *Breyer* [2016] EU:C:2016:779

Case C-345/17 *Buivids* [2019] EU:C:2019:122

Case C-673/17 *Planet49* [2019] EU:C:2019:801

DOCUMENTS FROM EU INSTITUTIONS

Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' WP 136

Article 29 Working Party, 'Opinion 15/2011 on the definition of consent' WP 187

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' WP 217

Commission, 'Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content' COM (2015) 634 final

European Data Protection Board, 'Guidelines 05/2020 on consent under Regulation 2016/679'

European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users'

European Data Protection Supervisor, 'Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (March 2014)'

European Data Protection Supervisor, 'Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content'

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on Data Protection Law* (Publications Office of the European Union 2018)

LITERATURE

Efroni, Z, 'Gaps and opportunities: The rudimentary protection for "data-paying consumers" under new EU consumer protection law' [2020] Common Market Law Review 799

Finck, M and Pallas, F, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR' [2020] International Data Privacy Law 11

Langhanke, C and Schmidt-Kessel, M, 'Consumer Data as Consideration' [2015] Journal of European Consumer and Market Law 218

Loos, M, Helberger, N, Guibault, L, and Mak, C, 'The Regulation of Digital Content Contracts in the Optional Instrument of Contract Law' [2011] European Review of Private Law 729

Mak, V, 'The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content' (Workshop for the JURI Committee 2016) <https://op.europa.eu/en/publication-detail/-/publication/6cfb903b-c295-11e6-a6db-01aa75ed71a1> accessed 21 April 2023

Metzger, A, 'Data as Counter-Performance: What Rights and Duties do Parties Have?' [2017] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 2

Metzger, A, Efroni, Z, Mischau, L, and Metzger, J, 'Data-Related Aspects of the Digital Content Directive' [2018] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 90

Metzger, A, 'A Market Model for Personal Data: State of Play Under the New Directive on Digital Content and Digital Services' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V* (Bloomsbury 2020) <https://ssrn.com/abstract=3666805> accessed on 29 April 2023

Narciso, M, 'Consumer Expectations in Digital Content Contracts – An Empirical Study' (2017) Tilburg Private Law Working Paper Series 1/2017 <https://ssrn.com/abstract=2954491> accessed 9 April 2023

Narciso, M, ''Gratuitous' Digital Content Contracts in EU Consumer Law' [2017] Journal of European Consumer and Market Law 198

Van Alsenoy, B, 'Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation' [2016]] JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 271

Voigt, P and vom dem Bussche, A, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017)