STUDY

Requested by the JURI committee

European Parliament

Update the Unfair Contract Terms directive for digital services

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 676.006 –February 2021

Update the Unfair Contract Terms directive for digital services

Abstract

This study analyses common terms in contracts of digital service providers, indicating when they could significantly distort the balance between the parties' rights and obligations to the detriment of consumers and should, therefore, fall within the scope of the Unfair Contract Terms Directive. Further, the study discusses the particularities of the assessment of online transparency of terms of digital service providers and sanctions they could face if they breach the current consumer protection framework. Recommendations are made to improve the effectiveness of this framework by: introducing a black and grey list of unfair terms, strengthening current sanctions, and introducing new obligations for digital service providers.

This document was requested by the European Parliament's Committee on Legal Affairs (JURI).

AUTHORS

Prof Marco LOOS, Professor of private law, in particular of European consumer law, University of Amsterdam, the Netherlands

Dr Joasia LUZAK, Associate Professor, University of Exeter, United Kingdom and University of Amsterdam, the Netherlands

ADMINISTRATOR RESPONSIBLE

Giorgio MUSSA

EDITORIAL ASSISTANT

Christina KATSARA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: Poldep-Citizens @ep.europa.eu

Manuscript completed in February 2021

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

ADR	Alternative dispute resolution
BGH	Bundesgerichtshof (German Federal Supreme Court in Civil Law matters)
CJEU	Court of Justice of the EU
CRD	Consumer Rights Directive
DCD	Digital Content Directive
DSP	Digital Service Provider
ECD	E-Commerce Directive
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
MD	Modernization Directive
UCPD	Unfair Commercial Practices Directive
UCTD	Unfair Contract Terms Directive

EXECUTIVE SUMMARY

Background

The Unfair Contract Terms Directive (UCTD) was adopted in 1993 before digital services became prevalent in modern society and prior to big data further exacerbating the contractual imbalance between digital service providers (DSPs) and consumers. Digital services have been defined in Article 2(2) Modernisation Directive (MD) as services that allow consumers to create, process, store or access data in digital form, or allow sharing of or any other interaction with data in digital form uploaded or created by consumers or other users of those services. These are, therefore, services accessed and provided in the online environment.

As the UCTD is a minimum harmonization directive and DSPs often provide their services cross-border, the current European framework against unfair contract terms may not be an effective consumer protection tool when consumers conclude contracts with DSPs. As a result of the Member States offering more consumer protection than what the UCTD provides for, DSPs may be confronted with a different assessment of unfairness in different Member States, creating an uneven level playing field for DSPs. The complex and varied national rules regarding unfair terms may also hinder the enforcement of the UCTD for national and cross-border enforcement agencies and consumer organizations.

Given the fact that the UCTD framework was developed for the offline world, this Study examines whether it is necessary to amend the UCTD to, on the one hand, improve consumer protection online against unfair contract terms of DSPs and, on the other hand, to provide more legal certainty to DSPs as to what terms and conditions are considered fair.

Aim

Despite previous attempts to revise the UCTD framework, e.g. during the works on the Consumer Rights Directive (CRD), the first change to it was introduced only in the past year, through the Modernisation Directive (MD). This change is limited to increasing the effectiveness of the UCTD sanctions and facilitating the enforcement of unfairness in the Member States.

This Study aims to propose measures increasing the effectiveness of the UCTD framework in the provision of digital services. To that effect, the Study presents an overview of commonly encountered terms used by digital service providers and evaluates whether they may cause a significant imbalance, contrary to good faith, in the parties' rights and obligations to the detriment of consumers. Where this is indeed the case, such terms could be considered unfair. This evaluation is conducted on the basis of the review of academic literature, case law, policy documents, news items reporting consumer problems with various digital service providers, as well as the study of actual terms of selected DSPs.

Key findings

The Study presents an overview of commonly encountered terms used by DSPs. It shows that many of these terms may indeed cause a significant imbalance, contrary to good faith, in the parties' rights and obligations to the detriment of consumers. In addition, the Study draws the attention to the fact that the assessment of unfairness may currently be hindered due to: 1) the UCTD framework having been adopted differently in the Member States as a result of its minimum harmonisation character; 2) no mention of online practices in the preamble to the UCTD and of how its general clauses could be applied to such practices; 3) an indicative-only list of possible unfair terms in the Annex to the UCTD; 4) the list of possible unfair terms not addressing issues commonly encountered in the digital world.

Amongst the problematic terms are terms having the object or effect of:

- misleading consumers as to the nature of the contract and statutory rights following from it (e.g. terms suggesting that: the contract is concluded for the provision of digital content rather than of digital services; a DSP acts in a non-professional capacity; the consumer protection framework does not apply);
- allowing DSPs to retain the collected personal data when consumers do not conclude a contract or the DSP terminates the contract or allowing DSPs to collect more personal data throughout the performance of the contract than what parties have originally agreed to, without the DSP notifying consumers about the change of the contract and giving them an option to terminate the contract;
- creating the impression that digital services are provided for free, where consumers are paying for the service with their personal data, time or attention;
- preventing consumers from withholding their performance;
- exempting the DSP from liability: 1) for consumers' damage caused by any illegal content posted on the DSP's website, if the DSP was informed of that content and did not remove it within a reasonable time, after which time the damage has occurred; 2) for consumers' damage caused intentionally or through gross negligence; 3) by creating the impression that services are provided "as is";
- allowing DSPs to modify terms, including price, where the contract does not provide a valid reason for the change of terms or the DSP did not inform consumers of the change with reasonable notice before the change was applied, or the consumer has not been informed about the option to and was not given a reasonable time to terminate the contract after having been informed of the change;
- hindering the consumers' use of the right of withdrawal;
- providing DSPs with a unilateral right to suspend the performance or terminate a contract, when the consumer's behaviour does not objectively justify this;
- preventing DSPs from making the data available to consumers after the termination of the contract, within reasonable time after the consumer has requested the termination;
- prohibiting or penalising negative reviews;
- preventing consumers from being able to contact a human contact point with their complaints and questions;
- infringing consumers' rights and data protection principles from the GDPR;
- creating an impression with consumers that their right to pursue judicial enforcement of their rights is limited or even excluded (e.g. by requiring arbitration; derogating from Brussels I Regulation (recast); by misinforming consumers as to their right to rely on the mandatory consumer protection of the country of their residence);
- discriminating against consumers as a result of the personalisation of such terms;
- limiting or excluding the access to digital services, if consumers do not give an explicit consent to the sharing of personal data in the scope exceeding what is needed for the provision of a digital service, including as a counter-performance for the provision of digital services;
- providing DSPs with a license to use the user-generated content unless this has been brought specifically to the consumers' attention at the moment of the contract's conclusion and has been individually, separately and explicitly accepted by consumers; and
- forming a no-survivor clause.

In the Study we elaborate on each of these types of terms and justify why they could be always or almost always considered unfair in consumer contracts. In the next paragraph we present our recommendations on how consumers could be protected against such terms drafted by DSPs.

It is important to note here that the Study shows that the contractual imbalance online will not be remedied simply by amending the UCTD. However, we conclude that the strengthening of the effectiveness of the UCTD framework could be achieved but only through the simultaneous revision of the UCTD, as well as the adjustment of certain obligations of DSPs in other EU consumer protection acts, e.g. in the CRD or in the forthcoming Digital Services Act.

Recommendations

In this Study, we recommend that the current indicative list of potentially unfair terms be turned into a black list of terms that under all circumstances should be considered unfair if these terms are included in a contract between a consumer and a DSP. This will provide better consumer protection, offer more legal certainty to DSPs, and help create a level playing field between DSPs.

In addition, we have identified several terms, listed in the paragraph on key findings, that currently are being used by DSPs that, in our view, are always or almost always unfair when used in contracts concluded with consumers, but that are not reflected or can only indirectly be linked to items on the current indicative list. We recommend that these terms should be placed on a black list of forbidden terms or on a grey list of terms presumed to be unfair if these terms are used in a contract with a DSP. Whether or not these lists should also be applied to other service providers than DSPs or other online traders, is of course a matter for political debate but is not discussed in this Study. We also recommend strengthening the sanction for the DSP's use of blacklisted terms by adding a paragraph to Article 6 UCTD. This paragraph should provide that where a DSP has used a blacklisted term, courts should be allowed to terminate the whole contract if this sanction is more advantageous for the consumer than merely removing the unfair term from the contract.

A third series of recommendations pertain to the conclusion of contracts and the incorporation of terms and conditions. First, we recommend that Article 1(i) of the Annex to the UCTD is re-drafted in order to explicitly mention that placing a hyperlink to terms and conditions somewhere on the DSP's website is insufficient to provide a 'real opportunity' of consumers being able to become acquainted with them before the conclusion of the contract. Instead, DSPs should have an obligation to draw the consumers' attention to such a hyperlink and they should have the burden of proof that this has, indeed, occurred. Consequently, it could be presumed that a disclosure of terms and conditions through a hyperlink, without the consumer having to tick a box or otherwise having to express consent explicitly, is non-transparent. This would be a rebuttable presumption.

Second, we recommend adopting an explicit prohibition of contracts being concluded by consumers providing a tacit consent online, which would disallow DSPs to rely on such contract types as browse-wrap. This will be achieved if DSPs are obliged to explicitly and clearly inform consumers that their action will lead to the contract's conclusion, before any such action occurs, and to ask for an explicit consumer's consent at that moment for the contract's conclusion. The consent could only be valid if consumers were given a real opportunity to read terms and conditions of the contract, prior to giving their consent, as well.

Third, we recommend obliging DSPs to promote transparency of online terms and conditions, of the mandatory consumer protection rules, and of the application of automated decision-making mechanisms. These information obligations could be added to the forthcoming Digital Services Act or a further revision of the CRD could be considered.

Finally, we would suggest the introduction at EU level of default rules regarding limitation of data storage for DSPs. Such rules would require DSPs to remove the collected consumer data within reasonable time from the moment such data becomes unnecessary for the provision of their services. Not regulating this on the EU level, will likely lead to the adoption of different time limits by the Member States, further contributing to the legal uncertainty on the market for the provision of digital services. Moreover, if the Member States do not adopt such rules and the contractual terms leaving the data storage open-ended or unreasonably long are considered unfair, the annulment of such terms would have detrimental consequences to consumers.

1. GENERAL INFORMATION

1.1. Protection framework of the UCTD

1.1.1. Unfairness test

The Unfair Contract Terms Directive (UCTD)[1] offers consumers (natural persons acting for purposes outside the scope of their business or profession) protection against contract terms that have been drafted in advance by the other party to a contract and that derogate, to the detriment of the consumer, from the otherwise applicable law. The UCTD is built upon the assumption that both with regard to their bargaining power and their level of knowledge, the consumer is in a weak position towards the trader. This leads the consumer to accepting terms without being able to influence their content (Micklitz 2010, pp. 360-361).[2] The UCTD provides that a contract term that is not individually negotiated may be reviewed in order to determine whether it is unfair (Tenreiro 1995, pp. 275-276).[3] Core terms – terms describing the main subject matter of the contract or as to the adequacy of the price and remuneration as against the services or goods supplied in exchange – are not subject to the unfairness test in so far as these terms are drafted in plain and intelligible language (Article 4(2) UCTD, see below, section 1.1.2). The notion of a core term is, however, to be interpreted restrictively.[4] It basically refers to a term that lays down the essential obligations of the parties and as such characterises the contract.[5] Terms that are ancillary to those that define the very essence of the contractual relationship can, therefore, not be seen as core terms.[6] Terms included in the Annex to the UCTD are by definition ancillary terms.[7]

Article 3(1) UCTD contains the criteria on the basis of which the court must ascertain whether or not a term is unfair: this is the case if the term is not individually negotiated and if,

> '*contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer*'.

Whether a term is part of terms and conditions or specifically formulated for this particular contract is immaterial, as long as it has not been the subject of negotiations with this particular consumer. However, if it is part of terms and conditions or otherwise drafted before the contract negotiations started, it is always considered to be not-individually negotiated (Article 3(2) UCTD). Whether a significant imbalance between the rights and obligations of the parties exists, is to be determined taking into account all circumstances of the case at the moment of the conclusion of the contract and all other terms of the contract (Article 4(1) UCTD). The national court is therefore required to take all terms of the contract into account when determining the unfairness of a specific term.[8] This implies, for instance, that when assessing the unfairness of a penalty clause, the court must take into account

1 Council Directive 93/13/EEC on unfair terms in consumer contracts [1993] OJ L 095/29 (Unfair Contract Terms Directive).

2 See for instance: judgment of 4 June 2009, Pannon, case C-243/08, EU:C:2009:350, paragraph 22; judgment of 26 April 2012, Invitel, case C-472/10, EU:C:2012:242, paragraph 33; judgment of 21 March 2013, RWE, case C-92/11, EU:C:2013:180, paragraph 41; judgment of 30 April 2014, Kásler, case C-26/13, EU:C:2014:282, paragraph 39.

3 Judgment of 21 March 2013, RWE, case C-92/11, C:EU:2013:180, paragraph 42; judgment of 30 April 2014, Kásler, case C-26/13, EU:C:2014:282, paragraph 40.

4 Judgment of 30 April 2014, Kásler, case C-26/13, EU:C:2014:282, paragraphs 42 and 49-50; judgment of 26 February 2015, Matei, case C-143/13, EU:C:2015:127, paragraphs 49 and 54; judgment of 23 April 2015, Van Hove, case C-96/14, EU:C:2015:262, paragraph 31.

5 Judgment of 3 June 2010, Caja de Ahorros y Monte de Piedad de Madrid, case C-484/08, EU:C:2010:309, paragraph 34.

6 Judgment of 30 April 2014, Kásler, case C-26/13, EU:C:2014:282, paragraph 50; Judgment of 26 February 2015, Matei, case C-143/13, EU:C:2015:127, paragraph 54; judgment of 23 April 2015, Van Hove, case C-96/14, EU:C:2015:262, paragraph 33.

7 See judgment of 26 February 2015, Matei, case C-143/13, EU:C:2015:127, paragraph 60.

8 Judgment of 21 February 2013, *Banif Plus Bank*, case C-472/11, EU:C:2013:88, paragraph 41.

the cumulative effect that the clause has together with other penalty clauses that are incorporated in the contract.[9] Circumstances that occur after the conclusion of the contract – e.g. in the case of a clause notably limiting liability, the actual magnitude of the damage sustained by the consumer and the degree of fault that can be attributed to the seller or supplier causing the actual damage – may not be taken into account when assessing the unfairness of the clause.

The good faith requirement in the unfairness test refers to the question whether the trader, dealing fairly and equitably with the consumer, could reasonably assume that the consumer would have agreed to such a term in individual contract negotiations.[10] Whether or not a term *significantly* disadvantages the consumer is to be determined by establishing to what extent the term derogates from the otherwise applicable provision of law.[11] A significant imbalance can already result from the fact that consumer rights under the contract are restricted, that the exercise thereof is constrained or that additional obligations are imposed on the consumer that were not envisaged by national law.[12] The unfairness may be taken away by a compensating advantage. However, it is often difficult to ascertain whether a particular advantage, such as a lower price, is actually related to an otherwise unfair term. The CJEU made clear that the mere fact that the contract term itself indicates that it is compensated by a lower price does not constitute proof of that relation.[13]

1.1.2. Transparency principle

Article 5, first sentence, UCTD provides that a term in writing must be drafted in plain, intelligible language. This sentence codifies the requirement of transparency with regard to contract terms in consumer contracts. The CJEU has made clear that this principle is to be interpreted broadly and that the mere fact that a term is formally and grammatically intelligible, does not mean that the term meets the requirements of transparency.[14] It requires the trader to draft a term in such a way that 'the average consumer' – who, in the words of the CJEU, '*is reasonably well informed and reasonably observant and circumspect*'[15] – would be able to determine, on the basis of clear, intelligible criteria, which economic consequences follow for them from the term.[16] The assumption is that the average consumer, who is expected to have read the terms before the conclusion of the contract, would then be able to determine whether they wish to be contractually bound by agreeing to the terms previously drawn up by the trader.[17] The consumer is not expected to possess legal knowledge. For this reason, a contract term indicating that the contract is governed by the law of Luxembourg without indicating that the consumer may also rely on the mandatory law of their country of residence, if the trader resides in that same country or targets its commercial or professional activities to that country, is not transparent.[18] Similarly, the French Tribunal de Grande Instance de Paris, in a collective action case against Google, held that a clause in the Terms of Use of Google + indicating that in some countries consumers may invoke mandatory national consumer protection rules and that Google +'s Terms of Use do not

[9] Judgment of 21 April 2016, *Radlinger/Finway*, case C-377/14, EU:C:2016:283, paragraph 95.

[10] Judgment of 14 March 2013, *Aziz*, case C-415/11, EU:C:2013:164, paragraph 69.

[11] ibid, paragraph 69; judgment of 16 January 2014, *Constructora Principado*, case C-226/12, EU:C:2014:10, paragraph 21.

[12] Judgment of 16 January 2014, *Constructora Principado*, case C-226/12, EU:C:2014:10, paragraph 23.

[13] ibid, paragraph 29.

[14] Judgment of 30 April 2014, *Kásler*, case C-26/13, EU:C:2014:282, paragraphs 71 and 72; judgment of 26 February 2015, *Matei*, case C-143/13, EU:C:2015:127, paragraph 73; judgment of 23 April 2015, *Van Hove*, case C-96/14, EU:C:2015:262, paragraph 40.

[15] The notion is developed in judgment of 16 July 1998, *Gut Springenheide*, case 210/96, EU:C:1998:369. It is also applied to unfair terms legislation, see judgment of 30 April 2014, *Kásler*, case C-26/13, EU:C:2014:282, paragraph 74.

[16] Judgment of 30 April 2014, *Kásler*, case C-26/13, EU:C:2014:282, paragraphs 73-75; judgment of 26 February 2015, *Matei*, case C-143/13, EU:C:2015:127, paragraph 74; judgment of 23 April 2015, *Van Hove*, case C-96/14, EU:C:2015:262, paragraph 41.

[17] Judgment of 23 April 2015, *Van Hove*, case C-96/14, EU:C:2015:262, paragraph 42.

[18] Judgment of 28 July 2016, *VKI/Amazon EU*, case C-191/15, EU:C:2016:612, paragraphs 66-71.

derogate from these statutory rights, lacked transparency and was therefore held to be unfair.[19] In our view, the court was right in deciding in this manner, as such a clause obscures the fact that the consumer is not informed of these mandatory rights and is rather lead to believe that the consumer protection rules have been respected by Google.

As the French case mentioned above already demonstrates, where a term is found to be non-transparent, this may be taken into account when determining whether the term is unfair.[20] For the unfairness test itself, however, it is not the circumstances of the average consumer but the circumstances of the specific consumer that must be taken into account.[21]

1.1.3. Indicative unfair terms list of the Annex

In addition to the unfairness test itself, Article 3(3) UCTD introduces '*an indicative and non-exhaustive list of the terms which may be regarded as unfair*'. The mere fact that a term is placed on this list does not mean that this term is deemed or presumed to be unfair.[22] However, the fact that the term is listed is '*an essential element on which the competent court may base its assessment as to the unfair nature of that term*'.[23] This implies that the national court must take account of the fact that the term is listed on the Annex; the fact that a term is placed on the Annex may therefore serve as a red flag to the court, signalling the potential unfairness of that term in a concrete case. However, given the fact that under the current text of the UCTD the evaluation of a term must always take into account the circumstances of the case, little certainty exists across the European Union as to the validity of the terms used by DSPs. Given the fact that these providers typically offer their services throughout the territory of the European Union, it could be argued that a uniform list of terms that under all circumstances should be regarded as unfair (a blacklist) would benefit legal certainty, enhance consumer protection and harmonise the level playing field for DSPs in the EU. This is true especially since the Modernization Directive (MD)[24] has introduced means for the enforcement of unfair terms legislation and thus removing unfair competition among service providers by using unfair terms towards consumers. In order to strengthen the effectiveness of these means, **we recommend** that the indicative list of potentially unfair terms be turned into a black list of terms that under all circumstances should be regarded as unfair, in particular in case these terms are used in a cross-border contract with a DSP.

1.1.4. Sanctions

Article 6(1) UCTD provides that if a term is found to be unfair, it is not binding on the consumer. On the basis of this provision, the CJEU developed two important streams of case-law. The first stream is the case-law according to which national courts are required to test unfair terms of their own motion.[25] This obligation for courts serves to replace the formal balance between the parties' rights and obligations laid down in the contract by a real balance that restores the equality between these

[19] TGI de Paris judgment of 9 April 2019, <https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/>.

[20] See judgment of 26 April 2012, *Invitel*, case C-472/10, EU:C:2012:242, paragraph 27; judgment of 28 July 2016, *VKI/Amazon EU*, case C-191/15, EU:C:2016:612, paragraph 68.

[21] Judgment of 14 March 2013, *Aziz*, case C-415/11, EU:C:2013:164, paragraph 68.

[22] Judgment of 4 June 2009, *Pannon*, case C-243/08, EU:C:2009:350, paragraphs 37 and 38; judgment of 9 November 2010, *Pénzügyi Lízing*, case C-137/08, EU:C:2010:659, paragraph 42.

[23] Judgment of 26 April 2012, *Invitel*, case C-472/10, EU:C:2012:242, paragraph 26.

[24] Directive (EU) 2019/2161 of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules [2019] OJ L-328/7 (Modernization Directive).

[25] See for instance judgment of 27 June 2000, *Océano*, joined cases C-240/98 u/i C-244/98, EU:C:2000:346, paragraphs 25-26; judgment of 4 June 2009, *Pannon*, case C-243/08, EU:C:2009:350, paragraphs 22-23 and 30.

parties.[26] The second stream pertains to the consequences of a term that is found to be unfair. In such a case, the term may not produce any binding effect on the consumer, implying that the court must leave the term out of consideration.[27] However, where the court has tested the term of its own motion, it is required on the basis of the principle of fair hearing to inform the parties to the dispute of the fact that it considers the term to be unfair and to offer the parties (in particular: the trader) the possibility to challenge that view.[28]

If, ultimately, the term is indeed found to be unfair, the court may not revise its content in so far as the contract may continue to exist without it. The reason for this is that otherwise the trader might be tempted to include potentially unfair terms, knowing that where the term is found unfair by a court, that court would revise or replace the term by a fair term. That would mean that the trader does not stand to lose anything by including unfair terms in the contract, and still benefits from the possibility that the term will not be challenged out of ignorance or because of the costs of litigation – which were the reasons why courts are required to test the term of their own motion in the first place. This would then compromise the chances of achieving the long-term objective of Article 7 UCTD – to prevent the continued use of unfair terms in consumer contracts – as the power of a court to amend the term would take away the dissuasive effect on traders of the straightforward non-application of unfair terms.[29] The court may not even substitute the term for the default rule that would have been applicable had the trader not included the unfair term in the contract.[30] This is different only if the contract could not continue to exist without such a substitution – as in that case the substitution of the term by the default rule would be in the interest of the consumer.[31] However, the protection of the consumer's interests does not go so far that the court would be required to annul or terminate the whole contract if such an action would be more advantageous to the consumer than merely leaving the unfair term out of consideration. Yet, given the minimum harmonisation nature of the UCTD, which follows from Article 8 UCTD, a Member State is allowed to determine that the whole contract is to be considered as void if this is more advantageous to the consumer.[32]

1.2. Digital services and unfairness

1.2.1. Concept of digital services

This Study follows the definition of digital services from Article 2(2) MD, which states that a digital service means:

> "*(a) a service that allow the consumer to create, process, store or access data in digital form; or*
>
> *(b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service*"

Consequently, digital services could only be services provided in the online environment by DSPs and not services that are provided offline, but solicited in the online environment. Examples of digital

[26] Judgment of 26 October 2006, *Mostaza Claro*, case C-168/05, EU:C:2006:675, paragraph 36; judgment of 4 June 2009, *Pannon*, case C-243/08, EU:C:2009:*350*, paragraph 31.

[27] See judgment of 14 June 2012, *Banco Español de Crédito*, case C-618/10, EU:C:2012:349, paragraph 65.

[28] Judgment of 30 May 2013, *Asbeek Brusse*, case C-488/11, EU:C:2013:341, paragraph 52.

[29] Judgment of 14 June 2012, *Banco Español de Crédito*, case C-618/10, EU:C:2012:349, paragraphs 65 and 69-70.

[30] Judgment of 21 January 2015, *Unicaja Banco*, joined cases C-482/13, C-484/13, C-485/13 and C-487/13, EU:C:2015:21, paragraph 32.

[31] ibid, paragraph 33.

[32] Judgment of 15 March 2012, *Pereničová*, case C-453/10, EU:C:2012:144, paragraph 36.

services are: file hosting services, social media, video and audio sharing services, games and other services offered in the cloud computing environment, webmail, cloud storage (Recital 19 MD).

At times, consumers may not be certain whether they have acquired a digital content or a digital service and, therefore, what protection they are entitled to. The MD recognises this ambiguity, as the supply of digital content could also be a series of individual acts of supply or even continuous supply throughout a period of time, which characteristics are normally associated with the provision of digital services (Recital 30 MD). Different consequences may follow from the distinction between the supply of digital content and of digital services. For example, consumers are entitled to the right of withdrawal in case they conclude a contract for the provision of digital services (Recital 30 MD). This will not apply if, instead, they arranged for a supply of digital content, not supplied on a tangible medium, and they have agreed that this supply should occur before the cooling-off period runs its course, explicitly acknowledging that they will lose their right of withdrawal.[33] To ensure effective consumer protection, Recital 30 MD recognises that in case of doubt as to what contract consumers have concluded, consumers should be offered the right of withdrawal applicable to the contracts for the supply of digital services.

A **recommendation** that could be made for the revision of the UCTD in this respect is a recognition of unfairness of such terms and conditions of DSPs, which do not transparently or correctly identify the nature of the contract, as well as statutory rights and obligations of parties following from it. Whilst this practice could give rise to a claim of an unfair commercial practice, it could also weigh in on the assessment of unfairness of terms and conditions.

1.2.2. Terms of service and privacy policies

As mentioned above, the UCTD assesses unfairness of not individually negotiated contractual terms. A contractual term is a term that determines the rights and obligations of the parties (Loos and Luzak, 2016, pp. 65-67). When a contract is concluded offline, consumers would either receive a document or a package of documents setting out such rights and obligations, or would be referred to them.[34] Similarly, in the online environment contractual terms may be placed on various websites of DSPs and they may also refer consumers to specific other documents, found elsewhere online.[35]

However, the online environment is more vast and may be perceived as more difficult to navigate without specific signposting. DSPs may easily separate various parts of their terms and conditions, and elaborate on them on different pages, under different headings. Whilst layering of information may be beneficial from the point of view of transparency (see further paragraph 3.1.2), consumers need to be able to recognise, which of the information available to them determines contractual rights and obligations. Whilst some headings would suggest it, e.g. if they refer to the terms of service, others are more ambiguous, e.g. a privacy policy. Some national courts might have already recognised, e.g. a privacy policy of iTunes as consisting of contractual terms and conditions, in a case against Apple.[36] The problem remains, however, that at the moment, DSPs do not clearly identify all contractual terms for consumers.

For example, on Twitter's homepage there are currently the following tabs that could lead consumers to documents containing contractual terms: "Terms of Service", "Privacy Policy", "Cookie Policy" and

[33] Article 16(m) Directive 2011/83/EU of the European Parliament and of the Council on consumer rights [2011] OJ L-304/64 (Consumer Rights Directive, CRD).

[34] E.g. such a reference may ask consumers to look up some of the contractual terms on the traders' website.

[35] E.g. codes of conduct placed on the website of a business association, to which the DSP belongs.

[36] Landgericht Berlin, judgment of 30 April 2013, 15 O 92/12 <www.vzbv.de/sites/default/files/downloads/Apple_LG_Berlin_15_O_92_12.pdf> accessed 4 December 2020.

"Ads info".[37] Dropbox has only a clearly marked tab "Policy" visible on the homepage. Upon clicking on it consumers may see tabs for "Terms of Service", "Privacy Policy", "Business Agreement", "DMCA Policy", "Acceptable Use" and "Open Source".[38] Could consumers, however, expect to find terms of service hiding behind a tab marked "Policy"? The main page of Discord, an instant messaging platform facilitating audio and video communication, contains a list of "Policies", where we may find a reference to "Terms", "Privacy", "Guidelines", "Acknowledgements" and "Licenses".[39] The homepage of Twitch, a live streaming service, has various tabs listed under the heading "HELP & LEGAL", none of them though mentions terms and conditions. However, if consumers click e.g. on "Cookie Policy" on that list, they will see a wide range of 21 further tabs: "Terms of Service", "Privacy Notice", "California Privacy Disclosure", "Community Guidelines", "DMCA Guidelines", "Trademark Policy", "Privacy Choices", "Trademark Guidelines", "Terms of Sale", "Developer Agreement", "Affiliate Program Agreement", "Supplemental Fees Statement", "Ad Choices", "Channel Points Acceptable Use Policy", "Bits Acceptable Use Policy", "Cookie Policy", "Photosensitive Seizure Warning", "Predictions Terms and Conditions", "Modern Day Slavery Statement", "Events Code of Conduct" and "Accessibility Statement".[40] This last example clearly shows how fragmented and complex the disclosure of online terms and conditions may be.

Therefore, it could be **recommended** that DSPs clearly identify what constitutes their terms and conditions. This could be done by including a clearly marked list of all the webpages containing contractual terms in one place, to which the homepage of a DSP should explicitly refer as that DSP's terms and condition (see also further in paragraph 3). This list could be accompanied by a short summary, an explanation as to what part of terms and conditions could be found under each heading, e.g. terms on performance of the service, price, liability.

1.2.3. Digital asymmetry: Consent and choice

In the following paragraphs we elaborate on various terms of DSPs, which could be assessed as unfair. We also indicate how the current European consumer protection framework against unfairness could be improved to address such unfair terms and conditions. The UCTD protection has been introduced to protect consumers from, in this case, DSPs being able to exploit the contractual imbalance of power between them and consumers by drafting unfair terms and conditions. Due to such an imbalance of power, consumers are placed in a 'take-it-or-leave-it' position when choosing a contract (Micklitz, 2010, pp. 360-361). This erodes their freedom of choice, which the UCTD does not aim to restore, but rather intends to provide a layer of substantive protection to consumers, as parties in a weaker transactional position.

A question could be posed whether such a consumer protection framework could ever be perceived as effective enough, considering that consumers may have even less choice to consent to specific online contracts than in an offline environment. This holds especially true, if DSPs are able to use big data to structurally exploit consumers' characteristics and preferences to push the acceptance of their services on consumers.[41] The external pressure will come not only from DSPs, but also from the society at large. For example, consumers whose family members and friends are on a particular social network (e.g. Facebook), will be exposed to social pressure to join the same network, to facilitate communication, sharing of news and events. Increased home-working during the Covid-19 pandemic

[37] Twitter website <https://twitter.com/home> accessed 13 November 2020.

[38] Dropbox website <https://www.dropbox.com/h> accessed 13 November 2020.

[39] Discord website <https://discord.com/> accessed 13 November 2020.

[40] Twitch website < https://www.twitch.tv/> accessed 13 November 2020.

[41] See further in paragraph 3.4 on digital vulnerability.

have likely forced many consumers to expand their use of cloud-based storage services, for both their professional and private purposes (Adshead, 2020). Often, consumers would join a particular file hosting service because their friends or colleagues wanted to share something on it with them. These few examples already show the societal pressure that consumers are exposed to when considering the conclusion of contracts for the provision of digital services.

It needs, therefore, to be explicitly stated that the purpose of adjusting the UCTD framework to sufficiently address the unfairness of terms offered by DSPs, would aim to ensure that consumers who succumb to such external pressures are not taken unfair advantage of. However, the introduction of this protection framework is unlikely to eliminate this pressure and restore consumers' free and real consent and choice online. The protection of consumers' consent and choice online could occur through the adoption of further safeguards in various other areas of European consumer law, competition law and data protection law.

2. (UN-)FAIR TERMS OF DIGITAL SERVICE PROVIDERS

2.1. Terms on conclusion of a contract

2.1.1. Browse-wrap contracts and tacit consent

Generally, in order for a contract to be concluded there needs to be a 'meeting of minds', i.e. a consent of both parties that they want to enter into a contractual relationship with each other on particular terms. This gives an expression to the principles of freedom of contract and party autonomy (Study Group on a European Civil Code and the Research Group on EC Private Law, 2009, p. 62). Whilst sometimes the consent may be implied, e.g. from parties' actions rather than words, it is a fundamental requirement of contract formation (Study Group on a European Civil Code and the Research Group on EC Private Law, 2009, pp. 567-568).[42]

In the online environment it may be more difficult to recognise when a consumer implicitly consented to enter into a contractual relationship on particular terms, which is one of the detriments of the indirect nature of the online communication between the parties. Contrarily, it may be much easier for DSPs to provide services to consumers, without having obtained an explicit consent from consumers to such an action. This was one of the reasons for the introduction of a specific disclosure obligation with respect to distance contracts for traders, which would lead to consumers explicitly recognising and agreeing to an order with an obligation to pay (Article 8(2) CRD). This provision will, however, not protect consumers in a situation when digital services are provided free of monetary charge, as at the moment the CRD does not recognise other means of payment, e.g. payment with data (see paragraph 2.6).

One of the new forms of contracting that emerged online is known as browse-wrap (Garcia, 2014, p. 31). Imagine a consumer browsing through the Internet, opening a website operated by a 'free' video streaming service provider, and opening one of the videos. The question that arises here is whether the DSP should be able to consider such a consumer's action as an implicit consent to the DSP's terms and conditions and, consequently, that a contract was concluded.[43] These terms and conditions are placed somewhere on the website of the DSP, could be accessed through a hyperlink and will regulate the relationship between the parties despite consumers likely never having seen them. It is highly likely that the consumer would just start to watch a video on a website without realising this might signify a consent to a contract's conclusion. In our view, the mere starting of the video should not be construed as implying consent to the conclusion of a contract. Instead, this commercial practice to a large extent mirrors what has been determined an aggressive commercial practice, prohibited by Article 5(5) and item 29 of Annex I to the Unfair Commercial Practices Directive (UCPD).[44] The validity of such 'contracts' is uncertain in several Member States (Loos and others, 2011, p. 736). In our view, rules similar to Article 7 GDPR[45] would fall short here. Under such an approach, DSPs would be required to warn consumers

[42] This may often occur when a contract is tacitly prolonged beyond its original duration, by parties continuing to perform their obligations.

[43] See e.g. Terms of Use of Veoh, an internet television company, stating: "By accessing or using the Veoh Service, you (…) are bound by the notices, terms and conditions in these TOU and, as applicable, elsewhere on www.veoh.com (including but not limited to our Privacy Policy and Copyright Policy, which are incorporated by reference). (…) If You do not agree to any of these terms and conditions, You may not use the Veoh Service." <https://www.veoh.com/corporate/termsofuse> accessed 12 November 2020. See also on Tinder's tacit consent: Forbrukerrådet, 'Complaint regarding unfair contractual terms in the Terms of Use for the mobile application Tinder' (3 March 2016) <https://fil.forbrukerradet.no/wp-content/uploads/2016/03/20160302-Complaint-Tinder.pdf> p. 2.

[44] Directive 2002/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L-149/22 (Unfair Commercial Practices Directive, UCPD).

[45] 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 [2016] OJ L-119/1 (General Data Protection Regulation, GDPR).

prior to any of their actions that would lead to a conclusion of a contract, even if it would be just upon opening a particular website. Such a warning should then transparently mention the fact that a contract is about to be concluded and provide a link to the DSP's terms and conditions. The reason why such an approach is not sufficient, is that even in the case of such a warning the consumer has no intention whatsoever to conclude any contract. This is different only if the consumer is not only warned, but is forced to accept that a contract is concluded in order to watch the video. It would, therefore, not be possible to imply consumers' consent to the provision of digital services (Gardiner, 2019, pp. 105-108). Moreover, even if such contracts are considered valid, uncertainty exists as to the incorporation of the terms and conditions (Loos and others, 2011, p. 737).

Whilst the risk of harm to consumers may be low when digital services are provided free of monetary charge, it is not completely eliminated. For example, accessing free digital services may expose consumers to digital security breaches. Providers of 'free' digital services might have limited or excluded their liability for such harms in their terms and conditions, which consumers are not even aware are applicable.

Therefore, we would like to make the following **recommendation**: a term that allows DSPs to consider a contract as concluded through browse-wrap contracting, should be perceived as unfair (blacklisted), even if there was no monetary payment foreseen for the provision of such a service.

Aside from explicitly acknowledging the intention to conclude a contract with DSPs, consumers could also be required to confirm that they have read and consented to their terms and conditions. Whilst empirical research proved that consumers tend not to read online terms and conditions (Bakos, Marotta-Wurgler, Trossen, 2014), subsequent studies emphasised the role that the increased transparency may still play in convincing consumers to pay attention to the online terms and conditions (Elshout and others, 2016). Therefore, a review of the UCTD framework could further investigate the transparency of the online terms and conditions (see further in para 3 below).

Moreover, to ascertain that consumers are only bound by terms that they actually could read and understand, we **recommend** that Article 1(i) of the Annex to the UCTD is re-drafted. Currently, this provision refers to such terms as potentially unfair, which are '*irrevocably binding the consumer to terms with which he has no real opportunity of becoming acquainted before the conclusion of the contract*'. The specificity of the online environment might require an addition to this provision. Namely, it could be explicitly mentioned that placing a hyperlink to terms and conditions somewhere on the DSP's website is insufficient to provide a 'real opportunity' of consumers being able to become acquainted with them before the conclusion of the contract. Instead, DSPs should have an obligation to draw the consumers' attention to such a hyperlink and they should have the burden of proof that this has, indeed, occurred. Consequently, it could be presumed that a disclosure of terms and conditions through a hyperlink, without the consumer having to tick a box or otherwise having to express consent explicitly, is non-transparent. This would be a rebuttable presumption.

2.1.2. Identity of the digital service provider

A common concern of consumers concluding online contracts is the lack of certainty as to who they are actually concluding a contract with. There are two facets to this problem. The first one relates to consumers' fear of fraud online, where the trader provides a false identity. This could be best mitigated by the robust enforcement of the national protection against fraud. The second one is based on consumers' misconception as to the identity of the online trader. This has been and could be further addressed by the European consumer protection framework. Consumers could be misled as to the DSPs' identity twofold. On the one hand, consumers may not be certain whether DSPs act in a professional capacity and, consequently, whether consumers may benefit from additional consumer

protection rights. On the other hand, consumers may not be clear as to who their contractual counterparty is for the provision of the digital services: a specific DSP or a platform facilitating the provision of such services.

Regarding the first issue, when consumers conclude contracts online they may not always be sure whether the party they conclude a contract with is acting in a professional or personal capacity, or even a mix thereof. It is important to be able to ascertain such capacity of the counterparty, as this will determine the scope of protection that the conclusion of a particular transaction brings with. This issue has already been discussed and addressed in European consumer law, e.g. Article 6(1)(b) CRD, pursuant to which online traders and service providers need to disclose their identity, such as their trading name. Moreover, item 22 in the Annex to the UCPD blacklists as unfair a commercial practice where the trader falsely claims or creates the impression that they are not acting for purposes relating to their trade, business, craft or profession, and instead falsely represent themselves as a consumer.

Regarding the UCTD framework we would **recommend** considering whether the current Article 1(b) of the Annex to the UCTD should not be extended to explicitly encompass as potentially unfair such terms and conditions of DSPs, which create an impression that they act in a non-professional capacity. This would indeed have the object or effect of '*inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier (…) in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations*'.

The platform economy further diminishes the clarity of the identity of the counterparty, as the platform itself may either be that counterparty or just act as an intermediary, with consumers not knowing who they are concluding a contract with (Recital 24 MD). The MD introduced, therefore, the concept of an 'online marketplace' to Article 2(1)(17) CRD, as an online service that allows consumers to conclude distance contracts with other traders or consumers. One of the new obligations that will follow for online marketplaces from Article 6a(1)(b) and (c) CRD will be to inform consumers whether third parties offering digital services on the online marketplace are professional parties, and if not, to warn that consumer rights will not apply to the concluded transaction. Commentators questioned the limited obligation of online marketplaces to confirm the veracity of the information provided by such third parties about the capacity, in which they are acting (Quarta, 2020). The platforms may simply rely on the declaration of that third party, which is aimed to assure compliance with Article 15(1) ECD.[46] It could, however, be feasible to request the platforms to do more here. We would **recommend** following the example of Article 14(3) European Law Institute Model Rules, which obliges platforms to examine the available transaction data to verify whether the trader's declaration was correct (Busch and others, 2020, p. 64).

Further, Article 6(1)(d) CRD obliges online marketplaces to inform consumers how any obligations towards consumers may be shared by them and by any third parties. We wonder, however, whether this will mean that consumers will be clearly informed that they may be entering into two separate contracts: one with the online marketplace (to which terms of use of that marketplace will apply) and the other with the third party (with the terms of use of the DSP being applicable) (Quarta, 2020, p. 4; Loos, 2019, p. 127). This does not seem to have been anticipated by the MD. As consumers are mainly focused on the conclusion of a contract for the provision of digital services, they may not even realise that they may have a contractual relationship with the online platform, as well. Therefore, it seems necessary to think about further enhancing consumer protection in this area. The previous **recommendations** (para 2.1.1) on obliging DSPs, including online marketplaces, to clearly identify the

[46] Directive 2000/31/EC of the European Parliament and of the council on certain legal aspects of information society services, in particular electronic commerce [2000] OJ L-178/1 (E-Commerce Directive, ECD).

moment of the contract's conclusion and highlighting its terms will be a good starting point to address this issue. Consequently, the online marketplaces, platforms facilitating the provision of digital services, should reveal their identity to consumers as one of their counterparties. This obligation would likely fit better in the forthcoming Digital Services Act[47] rather than in a revised UCTD framework.

2.1.3. Applicability of consumer protection framework to the agreement

The previous paragraph already illustrated the issue of the consumers' uncertainty as to whether they could count on being protected by the consumer protection framework when they acquire digital services. An introduction of specific disclosure obligations for DSPs and platforms will address this issue to an extent (see para 2.1.2). However, aside from a new duty for platforms to disclose when consumers are not awarded consumer protection, due to DSPs being consumers (Article 6a(1)(c) CRD), we would **recommend** the introduction of a general duty to inform consumers whether the mandatory consumer protection framework is applicable to their contract. Such a duty could be included in the Digital Services Act.

The protection will be further strengthened if DSPs and platforms refrain from adopting terms and conditions that could lead consumers to question the applicability of the mandatory consumer protection. For example, many DSPs adopt at the moment jurisdiction clauses, assigning jurisdiction over any disputes to overseas courts.[48] Such clauses would likely be unfair pursuant to the European consumer protection, e.g. Article 1(q) of the Annex to the UCTD, as they would '*exclude or hinder the consumer's right to take legal action or exercise any other legal remedy*'. After all, such a clause could discourage consumers from starting a legal action in their home country, to which they could be entitled pursuant Brussels I-Regulation (recast) (Loos and Luzak, 2016, 82-84)[49] (see also below, paragraph 2.10.2).

This is just one example of a situation, where a standard term of a contract for the provision of digital services could implicitly undermine consumer protection and discourage or even stop consumers from claiming their rights. We **recommend** protecting consumers in such situations through the application of Articles 1(b) and (q) of the Annex of the UCTD. However, at the moment these provisions are just indicative of unfairness and they are not expressly interpreted as applying to the situations mentioned in this paragraph. Consumer protection would be strengthened, if these provisions were decisive rather than indicative as to the unfair character of a standard term, i.e. if they were added to a black list of unfair terms (see also above, paragraph 1.1.3, and below, paragraph 4.1).

2.1.4. Payment arrangements

Consumers currently pay for digital services either via monetary means or with their personal data, time or attention (see paragraph 2.6). The method of payment for digital services with personal data of consumers has been explicitly recognised in Recital 24 and Article 3(1) DCD[50] as leading to a valid consumer contract conclusion, which entitles consumers to invoke rights and remedies provided for in this Directive. Another means of payment would be the situation where the consumer pays for the

[47] See on the Digital Services Act package e.g. European Commission's website: <https://ec.europa.eu/digital-single-market/en/digital-services-act-package> accessed 20 November 2020.

[48] See e.g. recognition of jurisdiction of the '*state and federal courts located in Las Vegas County of the State of Nevada*' in Veoh's terms of use <https://www.veoh.com/corporate/termsofuse> accessed 19 November 2020.

[49] Pursuant Articles 17-19 Regulation (EU) no 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L-351/1 (Brussels I-Regulation (recast)).

[50] Directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L-136/1.

digital service with their time by being exposed to advertisements exclusively in order to gain access to the digital service. Whereas contracts based on this business model are not covered by the scope of the DCD, Recital 25 DCD suggests that Member States are free to extend the scope of the act transposing the DCD to such situations. In this respect, it would be exceptional to gain access to digital services, which would not require any payment.

At the moment, Article 1 of the Annex of the UCTD mentions the following clauses that could give rise to unfairness regarding payment arrangements:

- (d) – *'permitting the seller or supplier to retain sums paid by the consumer where the latter decides not to conclude or perform the contract, without providing for the consumer to receive compensation of an equivalent amount from the seller or supplier where the latter is the party cancelling the contract';*
- (f) – *'(…) or permitting the seller or supplier to retain the sums paid for services not yet supplied by him where it is the seller or supplier himself who dissolves the contract';*
- (l) – *'providing for the price of goods to be determined at the time of delivery or allowing a seller of goods or supplier of services to increase their price without in both cases giving the consumer the corresponding right to cancel the contract if the final price is too high in relation to the price agreed when the contract was concluded'*.

None of these provisions is fully capable of addressing potential unfairness of a term of a contract with DSPs, which would regulate payment by consumers with personal data or by other means. However, when a consumer decides not to conclude or perform a contract or the DSP terminates a contract, we could argue that the personal data of the consumer that has already been shared, as part of a payment for the provision of digital services, should be erased pursuant to Article 17(1)(a) GDPR. We **recommend** for the UCTD framework to further clarify that Articles 1(d) and (f) of the Annex of the UCTD consider as unfair terms allowing DSPs to retain the collected personal data in the above-mentioned scenarios. This addition in the UCTD could create another legal ground for the DSP's erasure obligation of consumers' personal data regulated in Article 17(1)(e) GDPR.

Further, we **recommend** that Article 1(l) of the Annex of the UCTD is expressly extended to payment with the consumer's personal data. Then, it would be unfair for DSPs to increase the amount of personal data acquired from consumers, in addition to what has originally been agreed between the parties. We may think here of the recent German Facebook case, in which the *Bundeskartellamt* deemed Facebook to abuse their dominant position on the market by personalising users' experience on Facebook without an explicit consent (Podszun, 2019; Haucap, 2019). This personalised experience followed from Facebook starting to collect off-Facebook user data, i.e. data that users shared on apps other than Facebook. If Article 1(l) of the Annex of the UCTD applies here then such a change of the original 'price' for the provision of digital services should be clearly notified to consumers, giving them an option to terminate the contract, in order for the standard term that allows such a practice not to be seen as unfair (Loos and Luzak, 2016, pp. 68-72).[51]

Finally, we **recommend** that DSPs are obliged to transparently and in due time inform consumers that a digital service could only be provided to them upon payment, whether monetary or with personal data. Terms and conditions that refer to a free provision of a digital service, when in fact DSPs collect and process consumers' personal data, should be deemed as unfair (see paragraph 2.6).

[51] Following the preliminary decision of the German Federal Supreme Court, it seems that in order to avoid abusing their dominant position on the market Facebook will need to, however, also provide an option for its users to continue using Facebook without the personalised experience, which would create an additional obligation for digital service providers, see Decision of 23 June 2020, KVR 69/19, paras 120-121, 131.

2.2. Terms limiting/excluding the liability of digital service providers

2.2.1. Modification/ interruption of the digital service

DSPs often include a clause in their terms and conditions that states that services are provided "*as is*" (Bradshaw and others, 2011, p. 215; Rustad and Onufrio, 2012, p. 1126). The purpose of this clause is to exclude the online service provider's liability for any disturbance in the availability or reliability of the service and to ascertain that they give no guarantees with regards to the provision of their services. Indirectly, the clause, therefore, aims to exclude any liability by stating that the consumer could not reasonably expect the service to be rendered without disturbances. It may depend on a given national law whether such a clause would be considered or presumed unfair. It seems clear, however, that there will be circumstances, in which the service may not be available to the consumer due to the service provider's fault or negligence. In our view, terms excluding or limiting any liability of DSPs by stating the service is provided "as is" unfairly do not distinguish between disturbances caused due to the service provider's fault or negligence and disturbances caused outside the service provider's sphere of influence. For this reason, the French Tribunal de Grande Instance of Paris found that such a term in the terms and conditions of Google+ was unfair (Leone, 2019). Moreover, such terms do not respect the boundaries for a (permanent) *modification* of the digital service as provided for under Article 19 DCD. This provision requires DSPs to provide, i.a., a valid reason for a modification, and information to the consumer reasonably in advance on a durable medium of the features and time of the modification and of the right to terminate the contract or of the possibility to maintain the digital content or digital service without such a modification. For this reason, in our view a provision indicating that the digital service is provided "as is" is therefore in several ways misleading the consumer as to their statutory rights. **We recommend** that such a term is blacklisted as being unfair towards consumers.

It is worth mentioning here, that the French Tribunal de Grande Instance of Paris also declared another exemption clause in the terms and conditions of Google+ as unfair notwithstanding the fact that Google had added a clause indicating that the consumer may enjoy the application of national mandatory rules of consumer protection. This additional clause itself was held to be lacking transparency and was therefore held to be unfair.[52] In our view, the court was right in deciding in this manner, as such a clause obscures the fact that the consumer is not informed of these mandatory rights and is rather lead to believe that the consumer protection rules have been respected by Google.

Another question is whether the consumer should be allowed to withhold performance of their obligations – either payment of the price or supply of personal data, or both – in case the DSP's performance is interrupted or suspended, either because the digital service itself is not provided or because the DSP cannot provide the service as the digital content or the digital service needs to be modified. Recital 18 DCD leaves regulation of the matter expressly to the Member States. When such a right exists under national law, DSPs should not be allowed to circumvent that right by including a clause in their terms and conditions preventing the consumer from exercising such a right in case the DSP's performance is interrupted or suspended. For this reason, **we recommend** that clauses preventing consumers from exercising their right to withhold performance under national contract law are blacklisted.

2.2.2. Content moderation

Rather typical for digital services is the possibility for consumers (or users) to interact with the DSP and with other users on an online platform. Traders offering such services typically reserve the right to remove content posted by users when they consider that content to be a breach of contract by those

[52] TGI de Paris judgment of 9 April 2019, <https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/>.

users. However, some DSPs may explicitly refuse to monitor or control the content posted on their platform, and/or exclude all liability for content posted there.[53]

Where users are of course responsible for the content they post themselves, service providers cannot fully exempt themselves from liability for that consent if, after having been informed of the illegal content of posts (e.g. because posts are racist, sexist, defamatory or infringe copyright law) they do not remove such content. The 'safe harbour' provision of Article 15(1) ECD does not apply when the DSP is informed of illegal content posted on its platform, and the DSP may be required to terminate or prevent an infringement under Article 12(3), 13(2) or 14(3) ECD by order of a court or administrative authority. **We recommend** that a DSP should not be allowed to rely on a clause exempting the DSP from liability in case a consumer sustains damage after the DSP is informed of the illegal content of a post on its platform, and that a clause exempting the trader from liability in such case should therefore be blacklisted.

2.2.3. Unilateral modification of contract terms

DSPs often reserve the right to unilaterally amend the terms and conditions under the contract. The CJEU has set strict criteria under which such clauses may be allowed, in particular with regard to price amendment clauses. According to the Court, and in line with Articles 1(j) and 2(b), and 1(l) and 2(d) of the Annex to the UCTD price amendment clauses are valid only if a valid reason for the change of a term is specified in the contract, the trader is required to inform the consumer with reasonable notice before the change is applied, and the consumer is given a reasonable time to terminate the contract after having been informed of the change of the term, and the consumer is informed of that right at that time.[54]

Although all cases so far decided by the CJEU with regard to modification terms pertain to changes of the price or costs charged to the consumer, there does not seem to be a good reason not to apply the same reasoning to other unilateral changes of the contract, in particular, if they would substantially alter the parties' other rights and obligations (Leone, 2014, pp. 322-323). As there is no legal certainty on this point, and DSPs so far have neglected to amend their terms in response to the CJEU's case-law,[55] **we recommend** that the case-law of the CJEU should be codified and expressly applied to all unilateral amendment clauses.

2.2.4. Change of the service

The above-discussed unilateral right to modify contract terms differs from a right to modify services, but the second can be the result of the first, since adjustment of the contract terms may concern variation in the services' definition or scope. When consumers conclude a contract with an online service provider they expect to receive a certain service. If the service provider can unilaterally decide to change this service's scope or nature the consumer may be bound to a contract they might not have wanted.

A term enabling the DSP to unilaterally change the characteristics of the service is listed as potentially unfair under Article 1(k) of the Annex to the UCTD. However, Article 19 DCD sets boundaries for a change of the digital service as provided. These boundaries include that the DSP must have a valid

[53] See for instance the Twitter Terms of Service, as applicable to consumers living in the EU, EFTA countries and the United Kingdom, under 3, <https://twitter.com/home> accessed 20 November 2020.

[54] In particular judgment of 26 April 2012, *Invitel*, case C-472/10, EU:C:2012:242, judgment of 21 March 2013, *RWE*, case C-92/11, C:EU:2013:180 ; judgment of 30 April 2014, *Kásler*, case C-26/13, EU:C:2014:282.

[55] The terms used by Facebook, Google, Twitter and Dropbox have not been amended substantively in this respect since we published our paper, see Loos and Luzak, 2016, pp. 63-90 (pp. 80-81).

reason for the modification of the service, and that the consumer must be allowed to either terminate the contract without costs in case the change of the service is to their detriment and not-negligible, or to retain the digital service without modifications, and be informed of their right when the modification is notified to them. Under these conditions the term may indeed be considered fair. Since a derogation from the national provisions implementing the DCD to the detriment of the consumer is not allowed under Article 22 DCD, we do not see a need to introduce a term about this consumer right to the Annex of the UCTD, as well.

2.2.5. Data security

DSPs terms and conditions often include terms excluding liability for the loss of or damage to data supplied by or entrusted to the DSP. Data loss occurs when data is accidentally or deliberately deleted or made unavailable. It may be caused by an action of the DSP in response to (allegedly) illegal behaviour of the consumer, e.g. because the DSP discovers a photo which, according to the DSP, contains child pornography and subsequently deletes that data and possibly also other data of the same user stored on the DSPs servers. Whereas a DSP may be entitled to delete illegal data or make data unavailable in such cases, this is of course true only if the discovered data indeed was illegal. If, in fact, the photo was an innocent childhood photograph of the consumer themselves, this constitutes a breach of contract by the DSP for which the DSP is liable.

Data loss may also be the result of the operation of criminal behaviour of third parties, e.g. because ransomware or another computer virus has been downloaded on the consumer's hardware. Where the virus could be downloaded to a breach of data security on the part of the DSP – as the software used or provided by the DSP was not in accordance with the consumer's reasonable expectations, the DSP is liable as well (see also paragraph 2.9.4).

A term exempting the DSP from liability for the loss of or damage to the data or restricting such liability to cases of intent or gross negligence falls within the scope of Article 1(b) of the Annex to the UCTD and is thus potentially unfair within the meaning of Article 3(1) UCTD. In previous work (Loos and Luzak, 2016, pp. 80-81), we have discussed clauses used by Facebook, Twitter, Google, and Dropbox excluding liability for data or financial losses, or for indirect, special, consequential, exemplary, or punitive damages, or by capping their liability for such loss. We concluded that even though these clauses fall within the scope of the provision in the indicative list, there is no general indication of the acceptability of such terms under current EU law (Ebers, 2021, pp. 17-18).

For this reason, **we recommend** clearer rules indicating which exemption clauses may and which may not be used, in particular by blacklisting clauses that exempt the DSP from liability in case of damage caused intentionally or through grossly negligent conduct, e.g. by not providing updates of the digital content or the digital service in accordance with Article 8(2) DCD within a reasonable time after the DSP has or should have discovered the lack of conformity.

2.3. Terms on the right of withdrawal

The right of withdrawal entitles consumers to annul a distance contract without having to provide any reasons and free of charge, pursuant to Article 9(1) CRD. This right applies in distance contracts in order to protect consumers against an informational disadvantage they suffer, when compared to a purchase in a physical store (Luzak, 2014). Namely, consumers purchasing services online are not able to as easily ascertain the nature of such services.[56]

[56] Recital 14 Distance Selling Directive, Directive 97/7/EC [1997] OJ L144-19.

As it has been mentioned in paragraph 1.2.1, Recital 30 MD specifically clarified that consumers who conclude a contract for the provision of digital services are entitled to the right of withdrawal. The 14-days cooling off period enables them to test the digital services and decide whether to keep the contract. This provision mentions now also the 'continuous involvement of the service provider' with the provision of digital services as justifying the application of the right of withdrawal to such contracts.

Article 16(m) CRD excluded from the distance contracts awarding consumers a right of withdrawal contracts for the supply of digital content, which is not supplied on a tangible medium, in specific situations. Namely, where consumers expressly agreed to the immediate performance of the contract and acknowledged that they would lose their right of withdrawal when the performance begins. Recital 30 MD has clarified that this exception does not apply to contracts for the provision of digital services, where consumers request their immediate provision.[57] However, some contracts may lead to uncertainty whether they pertain to the supply of digital content or of digital services. Therefore, Recital 30 MD now expressly states that in case of doubt as to what contract consumers have concluded, for the provision of digital services or of digital content, consumers should be offered the right of withdrawal applicable to the contracts for the supply of digital services.

For example, when a consumer subscribes to an online gaming server, joining an online gaming session, which would require streaming of the video and audio content, this would likely be perceived as a provision of a digital service. It would not matter that a consumer did this only once and logged out within a few minutes. This consumer could then use the right of withdrawal even if they expressly requested immediate provision of the service. However, if the same online gaming server will allow a direct download of a game to the consumer's computer, this would likely be seen as a supply of digital content. Again, it would be irrelevant whether a consumer downloaded many games over a period of time or just one game. In the case of contracts for the supply of digital content, consumers could then explicitly consent to lose their right of withdrawal when they requested an immediate download.

A distinction should be made for a situation where consumers consent to the provision of paid digital services during the cooling-off period and these services are provided in full. DSPs will then need to require consumers expressly requesting such an immediate performance and expressly acknowledging that they will lose their right of withdrawal upon the full performance of the contract, pursuant to the new Article 8(8) CRD, as modified by the MD. The right of withdrawal in such a case is then excluded, pursuant to Article 16(a) CRD. This provision protects DSPs, where they allow consumers to conclude short-term contracts, e.g. to facilitate a transfer of big files (see e.g. the services of WeTransfer Pro).

As the above-discussed provisions introduce mandatory consumer protection, DSPs may not deviate from them in their terms and conditions. However, we can imagine that some terms of DSPs could obstruct consumers from making use of their right of withdrawal. We would **recommend** to consider as unfair any terms of DSPs that would hinder the consumers' use of the right of withdrawal.

For example, it needs to be emphasised that a consequence of classifying the contract as one for the provision of digital content rather than digital services, obstructs the application of the consumers' right of withdrawal, introducing more limitation to the exercise of this right. Therefore, terms that would mislead consumers as to the object of the contract should be considered unfair. Further, despite consumers not having an obligation to give a reason for their withdrawal from the contract, DSPs may inquire about it, possibly creating an impression with consumers that there needs to be a 'justifiable' reason for such a withdrawal. Additionally, it could hinder consumers to make use of their right of withdrawal, if it were difficult to communicate this to the DSP in question or if the model withdrawal

[57] See e.g. Terms of Service of WeTransfer Pro, clause 8.2 <https://wetransfer.com/legal/terms> accessed 20 November 2020.

form was not easily found on the DSP's website.[58] Finally, as consumers should be able to use the right of withdrawal without having to pay any charges, asking them to pay any compensation or damages to DSPs should constitute an unfair term.

2.4. Terms on suspension/ termination of contract

2.4.1. Events triggering the suspension/ termination

Some DSPs regulate in their terms and conditions which events entitle the DSP to suspend performance of their obligations under the contract or to terminate the contract as a whole. The most common examples pertain to the situation where the consumer does not perform their core obligations under the contract, e.g. by not paying the price in money or by not providing personal data in a case where that personal data constitutes the consumer's counter-performance. Since such provisions do not derogate from the default rules otherwise applicable to the contract, they will not be considered as unfair.

Terms and conditions are, however, also used to extend the number of events triggering the suspension or termination of the contract in case of a breach of contract of secondary obligations of the contract. Such terms may be justified in case of illegal behaviour of the consumer, e.g. because the consumer stores illegal content on the DSP's servers, or in case of other serious reasons. However, where the consumer's behaviour does not objectively justify suspension or termination, introducing the possibility for the DSP to unilaterally suspend performance or terminate the contract amounts to a discretionary power for the DSP to free itself from its obligations under the contract. Such a term then falls within the scope of Articles 1(f) and 1(g) of the Annex to the UCTD and is thus potentially unfair within the meaning of Article 3(1) UCTD. **We recommend** that such clauses be forbidden.

2.4.2. Survival and recovery of data stored/shared/created

When the contract between a consumer and a DSP is terminated – either by the consumer or the DSP – the consumer should be enabled to recover the data stored, shared or created by them. Article 16(4) DCD introduces a right for the consumer to request the DSP to make the digital content available to them in case of a failure to supply the digital service, a lack of conformity of the digital service, or a modification of the digital service that is not accepted by the consumer. A term restricting such right would be in direct violation of the DCD and therefore in breach of Article 22 DCD and thus not be binding on the consumer.

There are, however, other instances where the contract between consumer and DSP may be terminated. First, the parties may have concluded a contract for a determined period of time. When that time has elapsed, and the contract is not extended, it is terminated automatically. Second, the contract may be terminated by the DSP for breach of contract by the consumer. And finally, the contract may be terminated automatically under national law in case of a contract where the consumer merely undertook to provide personal data to the DSP but subsequently withdraws consent for the processing of personal data.[59] There is no reason why in these cases the consumer should not be able to have recovered the digital content from the DSP as well as their personal data, following the GDPR

[58] E.g. we could not find the model withdrawal form on the WeTransfer website < https://wetransfer.zendesk.com/hc/en-us/articles/360023804571-How-to-cancel-your-WeTransfer-Pro-account> accessed 20 November 2020. Previously, the Norwegian Consumer Council noted that in the video game industry it was very difficult if not impossible for consumers to withdraw from contracts for pre-ordered video games, see Forbrukerrådet, 'Nintendo breaking the law' (21 February 2018) <https://www.forbrukerradet.no/side/nintendo-breaking-the-law/> accessed 20 November 2020.

[59] This is for instance the case under Article 7:50ab(5) Dutch Civil Code (draft), which is to be introduced by the draft-bill transposing the DCD into Dutch law.

(see paragraph 2.9). Since this has not been explicitly regulated under the DCD, DSPs may try to use their terms and conditions to pre-emptively exclude their obligation to make the digital content available to the consumer in such cases. For this reason, **we recommend blacklisting** terms allowing or enabling a DSP not to make data available to the consumer after the termination of the contract within a reasonable time after the consumer's request.

2.5. Terms on digital inheritance

DSPs often not only restrict the possibility for consumers to transfer the rights they receive under the contract to third parties, but even try to exclude these rights from the consumer's inheritance in case the consumer dies. For that purpose the contract contains a so-called 'no survivor' clause. For example, Article IV under D of the general terms and conditions for the i-Cloud, Apple's online storage service,[60] stipulates the following:

> '***D. No Right of Survivorship***
>
> *Unless otherwise required by law, you agree that your Account is non-transferable and that any rights to your Apple ID or Content within your Account terminate upon your death. (...)'*

Linden Lab's Second Life Terms and Conditions for the game Second Life[61] also contain such a clause. With respect to the 'Linden dollars', the virtual currency of the game, Article 3.1 of Second Life Terms and Conditions provides:

> '*Except as expressly permitted by this Second Life Policy or otherwise expressly permitted by Linden Lab, Linden Dollars may not be sublicensed, encumbered, conveyed or made subject to any right of survivorship or other disposition by operation of law or otherwise, and you agree that any attempted disposition in violation of these Terms of Service is null and void.*'

Article 3.4 provides for a similar provision regarding 'Virtual land', which refers to the graphical representation of the three-dimensional virtual world space. Both the currency and the land therefore perish upon the death of the consumer.

Whereas we understand that a DSP may want to exclude the possibility for a consumer to actively transfer the rights under the contract to a third party – which would effectively mean that the DSP would have a new creditor with regard to the digital service that is to be provided – we see no generally applicable valid reason why a DSP should be allowed to also ban the transfer of a consumer's rights under the contract which is the result of the operation of the rules on inheritance law. However, we do not rule out that such a clause could be acceptable in the case where the personal capabilities and performance of a consumer is determinate for the accumulation of content and affects the position of other consumers. This can, for instance, be the case in multiplayer games played online where the personal performance of the consumer has an impact on the position of other participants in the game. For cases in which data accruing to the consumer has been stored (as in the case of cloud storage) or in which a form of virtual ownership has been assigned to the consumer (as in the case of Second Life), this seems less likely to us, because it is not immediately visible which legitimate interests of the DSP or third parties are at stake. However, even then, if there would be interests that could justify the exclusion of the transfer of rights to heirs, such clauses should be allowed. For this reason, **we recommend** to place no-survivor clauses on a grey list, which means they will be presumed unfair

[60] We have used the Irish version of the terms <https://www.apple.com/ie/legal/internet-services/icloud/en/terms.html> accessed 21 October 2020. A similar provision is included in clause 25 (General information, at the very end of the clause) of the Terms of Service <https://www.arlo.com/uk/about/terms-and-conditions/> accessed 21 October 2020.

[61] See <https://www.lindenlab.com/legal/second-life-terms-and-conditions> accessed 21 October 2020.

unless the DSP provides a valid reason to exclude the transfer of benefits in case of the death of the consumer, which reason should already be indicated in the contract.

2.6. Terms addressing the 'free' character of digital services

As we have mentioned in paragraph 2.1.4, consumers frequently pay for the provision of digital services through other than monetary means. Mainly, we would expect the DSPs to collect and process consumers' personal data. Such data may then be used, e.g. to create email marketing lists, which are then utilised for further advertising. However, DSPs may also rely on other business models, where consumers would pay for the digital services with their time and attention. DSPs could then earn money either based on consumers' clicks on various advertisements displayed to them or through the cost-per-mille display advertising mode.[62]

Moreover, DSPs may use a freemium (or an in-app purchase) revenue model, where they provide consumers with access to some digital services for free, but further services or digital content is limited or blocked.[63] DSPs would gain consumers' attention originally by making a 'free' offer, hoping to develop consumers' loyalty and engagement, which could stop consumers' from declining paid content further down the line (Shi, Xia & Huang, 2015).

When consumers pay for digital services with their personal data, time or attention paid to advertisements, the question may arise whether DSPs could draft different, more onerous terms for these contracts when compared to terms drafted for digital services for which consumers pay with money. Recital 24 and Article 3(1) DCD explicitly recognise that consumers concluding contracts, where the payment occurs by data, and therefore where the personal data is a counter-performance (Helberger, Zuiderveen Borgesius, and Reyna, 2017, p. 1446), are encompassed by the protection of the DCD. Undoubtedly, when such contracts contain not individually negotiated terms and conditions, such terms also fall under the purview of the UCTD. Other types of payment, e.g. with consumers' time and attention, have not yet been explicitly addressed by the European legislator. This raises questions, therefore, what standard of assessment should be applied in the evaluation of the unfairness of the terms and conditions of DSPs providing their content in exchange for other than monetary payments (Helberger, Zuiderveen Borgesius, and Reyna, 2017, pp. 1447-49).

As we outlined in paragraph 1.1.1, the unfairness test requires an investigation whether a given term caused a significant imbalance between the parties' rights and obligations, contrary to good faith, and to the detriment of consumers. As consumers are still providing counter-performance – their personal data, time and attention – to DSPs upon the contract's conclusion, such a significant imbalance could occur if DSPs did not accept any, or significantly fewer, obligations towards consumers for the provision of the digital services in exchange of other than monetary payments. This could occur when DSPs would, e.g. adopt terms excluding or limiting their liability for the quality and continuity of the provided services (see also paragraph 2.2) or for the security of the consumers' data (see also paragraph 2.9).

We are not aware of any studies outlining the differences and similarities in DSPs' profits when they use various, above-mentioned business models. However, we know that data, time and consumers' attention all have value and that DSPs are not paying consumers for any of their above-mentioned contributions by means other than the provision of digital services (Mitchell 2018). Moreover, DSPs continue to sustain the illusion that consumers' contribution other than monetary payment is unimportant.

[62] Where the advertisers are charged a fixed price per each 1.000 'impressions' an ad receives, with impressions referring to views.
[63] This is a business model of many popular DSPs, e.g. Candy Crush, Spotify, Tinder, WordFeud.

For example, Facebook's Terms at the moment specify that

> '*instead of paying to use Facebook (…) you agree that we can show you ads that business and organisations pay us to promote (…). We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you.* (…)'.[64]

This creates an impression that it is not Facebook users who pay for the digital services, but rather other businesses. A further example may be found when we look at Spotify's End User Agreement, which in clause 3.1 states

> '*(…) The Spotify Service that does not require payment is currently referred to as the "Free Service".*"[65]

However, users of the 'Free Service' of Spotify are exposed to advertisements, which means they actually pay for these 'free' digital services, with their time and attention to such advertisements.

In all the above-mentioned cases, it could be argued that online terms and conditions referring to the free provision of the digital services could be misleading and possibly also unfair. As long as the business model of online DSPs relies on a contribution or an activity of consumers, it could be argued that the digital services are not provided for free. Therefore, we would **recommend** to consider terms creating an impression that the provision of the digital services is free as unfair. Consumers' non-monetary payment should be explicitly acknowledged by DSPs. Moreover, we would **recommend** that payment in data is explicitly recognised as one of the obligations of consumers that are weighed when determining the balance between parties' rights and obligations in the unfairness test.

It is worth noting here, that previously the French Tribunal de Grande Instance of Paris declared as unfair some terms of Google+ service, amongst others because they did not make consumers aware of the fact that the personal data collected by Google+ had a commercial value and would be used for commercial purposes (Que Choisir, 2019).[66] Further, in May 2019 collective actions have been filed against Facebook not protecting the personal data from being shared with third parties by various national consumer organisations, e.g. Belgian, Italian, Portuguese and Spanish ones (BEUC, 2018). So far, only the Lazio Regional Administrative Court in Italy has issued a judgment supporting the decision of the Italian Competition Authority. In this decision the Italian court recognised the commercial value of data and condemned Facebook for claiming to provide its services for free (Kulesza, 2020).

2.7. Terms following from the personalisation of digital services

2.7.1. Presence of automated decision-making mechanisms

DSPs just like other online traders may use various automated decision-making mechanisms, to personalise either provision of their digital services or of the sponsored advertisements, which finance their services. The use of automated decision-making and profiling of consumer behaviour has so far only been recognised in Recital 45 MD within European consumer law. This provision draws attention to DSPs gaining insights as to consumers' purchasing power, which allows them to personalise prices (see further paragraph 2.7.2). However, it is important to note that acknowledging the impact of automated decision-making on pricing practices, covers only a small part of the usefulness of such mechanisms for online traders. Collected big data on consumers' behaviour, characteristics and

[64] <htittps://www.facebook.com/legal/terms/update> accessed 20 November 2020.

[65] <https://www.spotify.com/uk/legal/end-user-agreement/#s3> accessed 20 November 2020.

[66] The text of the judgment is available on the Que Choisir's website.

preferences may also impact conditions, under which digital services would be provided, as well as determine the access of consumers to digital services to begin with, e.g. via geoblocking.[67]

Consequently, the fact that DSPs use automated decision-making mechanisms may have a significant impact on both the contract's conclusion and its terms. We **recommend**, therefore, that the obligation to disclose the use of automated decision-making mechanisms is broadened for online traders, including DSPs. DSPs should be obliged to disclose fully how the use of automated decision-making impacts the provision of digital services. This could be addressed in the forthcoming Digital Services Act. A consequence of introducing such an obligation for DSPs, could be that when they are in breach thereof, any terms that have been personalised through the use of automated decision-making, but not disclosed to consumers as such, could be considered unfair and, therefore, non-binding.

Moreover, the European Parliament has already drawn attention to the fact that consumers should not only be informed about how the automated decision-making systems work, but also '*about how to reach a human with decision-making powers, and about how the system's decisions can be checked and corrected.*'.[68] We **recommend** explicitly recognising the obligation of DSPs to facilitate such human contact points for consumers and human oversight over the automated decision-making. If DSPs terms and conditions envisage only providing consumers with a contact option through the use of virtual assistants and chatbots, this could be considered an unfair term.[69]

2.7.2. Price and terms discrimination

The possibilities of online price discrimination or consumers being offered different contractual terms as a result of recognising consumer preferences have long been discussed in the EU (Schulte-Nölke and others, 2013). Even before the widespread use of sophisticated algorithms allowed online traders to build detailed customers' profiles, it was acknowledged that the sole fact that they could identify the consumers' country of purchase could allow, e.g., the introduction of various prices for the same product in different Member States (Schulte-Nölke and others, 2013). The availability of big data exacerbated the possibility of discriminating against online consumers on the basis of price or terms. However, there is not yet conclusive empirical evidence of such discriminatory practices (Bourreau and de Streel, 2020).[70] What economists have showed was that DSPs could increase their revenue if they applied price discrimination (Shiller, 2014), i.e. that it would be profitable for them to use such discriminatory practices.

Recital 45 MD indicates the need to introduce a new obligation for online traders to inform consumers about any price personalisation that might have occurred on the basis of automated decision-making. The new Article 6(1)(ea) CRD introduces such an information duty for online traders, including DSPs. Therefore, any time insights into consumer behaviour will lead to a price adjustment for the digital services, consumers will need to be informed of that fact. There is, however, no specific requirement for this information to reveal the algorithm and its methodology, which has led to a specific price adjustment and possibly even price discrimination. DSPs will also not need to provide comparative pricing information, i.e. to reveal how the price has been adjusted for a particular consumer (Reyna, 2019). This will hinder the finding of any price discrimination.

[67] The latter issues has partially been dealt with through the adoption of Regulation (EU) 2018/302 on addressing unjustified geo-blocking and other forms of discrimination [2018] OJ LI-60/1.

[68] Resolution on automated decision-making processes: ensuring consumer protection and free movement of goods and services, 2019/2915(RSP).

[69] Such a practice could also be contrary to Article 22(1) GDPR.

[70] There is mostly anecdotal evidence of some price discriminatory practices online:

<https://en.wikipedia.org/wiki/Criticism_of_Amazon#Differential_pricing> accessed 20 November 2020.

Moreover, the MD does not introduce a duty to inform consumers that automated decision-making mechanisms have been used by DSPs, and other online traders, to alter contract terms other than the price (see our recommendation in the previous paragraph). We pose the question here whether the UCTD framework should be utilised to prevent any discrimination as to price or contract terms from happening, when DSPs use automated decision-making.

For example, we could **recommend** considering as potentially unfair such terms of DSPs, which have been adjusted as a result of automated decision-making for a given consumer, without this having been disclosed to consumers. Moreover, the assessment of unfairness of a given term could account for whether it has been personalised. A rebuttable presumption could be introduced that personalised prices[71] and terms are discriminatory, and, therefore, unfair.

Therefore, despite the fact that personalised pricing is usually thought about as being better addressed by the framework of the UCPD, there could be a role here for the UCTD to play, as well.

2.7.3. Persuasion profiling

Aside from adjusting terms of contract based on the information collected about consumers, DSPs could use automated decision-making to steer consumers in the online environment by disclosing to them only specific offers, or adjusting the order in which offers are displayed (Mattioli, 2012; Bourreau and de Streel, 2020). The personalised ranking of offers is a relatively common commercial practice (European Commission, 2018). Through such practices, DSPs utilise collected big data not to adjust prices and terms of a contract to individual consumers, but rather to entice them to conclude a contract with a given DSP or to use specific digital services of a particular provider.

For example, Netflix learns which movies to recommend to their users, Google adjusts search and news results, etc. (Kaptein, 2015). Considering that persuasion profiling works best if it is invisible, DSPs may argue that the introduction of an obligation to disclose such practices will directly undermine their effectiveness. Still, Recital 18 MD recognises that a higher ranking or a more prominent placement given to particular offers in online search results has an important impact on consumers. Following Recital 20 MD, Annex I to the UCPD has been adjusted to consider it an unfair commercial practice when online traders do not disclose that certain offers have been positioned higher or better in search results following a payment to that effect from their providers.

It is important to note that the introduced provisions seem to target a situation where DSPs would facilitate a search option for products and services of various other online providers, as there is a requirement of payment by a trader to the DSP facilitating the search. This excludes, therefore, DSPs using persuasion profiling to promote some of their own services, as in the above-explained Netflix example.

Recently, the German Federal Supreme Court (*Bundesgerichtshof*, *BGH*) issued a preliminary decision supporting the decision of the German Federal Cartel Office (*Bundeskartellamt*), establishing that Facebook abused their dominant position on the market of social networks (Podszun, 2020).[72] Namely, Facebook collected and processed users' data shared on and off-Facebook to provide their consumers with a personalised experience. As *Bundeskartellamt* and *BGH* both ascertained consumers had no choice to refuse collection of such off-Facebook data and the provision of the personalised services, without giving up access to Facebook services altogether.[73] These decisions emphasised the value of

[71] Where the use of automated decision-making is not disclosed to the consumer, the price - which is not individually negotiated - lacks transparency and is thus subjected to the unfairness test under Article 4 UCTD.
[72] Decision of BGH of 23 June 2020, KVR 69/19.
[73] Ibid, paragraph 58.

consumers' choice, which could lead to the obligation of DSPs not to provide tied services, but rather to allow consumers to decide the level of data they wanted to share, and consequently the level of the personalisation of provided services.[74]

The German case shows that competition law may be used to help preserve consumers' choice when DSPs use big data to personalise their own services. However, as competition law likely stepped in here due to the missing provisions of the consumer law framework, and because Germany has a very robust Federal Cartel Office, it might be worth considering whether the UCTD could address persuasion profiling. The UCPD may be easier engaged here. Namely, if DSPs tie digital services, which could be offered separately, and where the tying of these services would lead to the increase in consumers' personal data collection, this could be considered an unfair commercial practice. Further, however, we would **recommend** that contractual terms not offering consumers a choice to access digital services of a given DSP, without agreeing to sharing of their personal data in the scope exceeding what is needed for a provision of a given service, should be presumed to be unfair (see also paragraph 2.9.1). We should explain here that we consider as 'necessary for the provision of a given service' also the situation where consumers provide personal data as counter-performance for the DSP's provision of the digital service, provided that the consumer has expressly consented to the provision of the personal data for this purpose. The DSP should then describe in as precise terms as possible, however, the scope of the personal data they will be collecting as counter-performance.

2.7.4. Standardised character of terms

Whilst DSPs and online traders may increasingly use big data to personalise the provision of their services, questions could be raised whether this could threaten the applicability of the UCTD framework to online terms and conditions.

As we have mentioned in paragraph 1.1.1 the UCTD applies to terms that have not been individually negotiated. If a DSP personalised their provision of services and perhaps also their contractual terms for individual consumers, this could perhaps eventually take away the standardised character of such terms, but we would argue that it does not make them individually negotiated.

To start with, it needs emphasising that at the moment any personalisation of terms will likely still occur in a standardised way. This means that DSPs would use insights into given consumers' behaviour and preferences, to group consumers into specific categories. They would then prepare templates of different terms and conditions, including of prices, for each of these consumer groups (Luzak, 2021). The reason for this partial personalisation is that most DSPs would not have access to enough big data nor yet have found a way to efficiently adjust their business to individual consumers. As a result, the terms would still be standardised, however, on a different granular level.

More importantly, however, personalised terms are not synonymous with individually negotiated terms. As the CJEU previously emphasised, individually negotiated terms require a real opportunity being provided to consumers to influence the content of such terms, and, therefore, it does not matter if the terms have been prepared for the purpose of a specific contract.[75] Especially if they have been prepared in advance, they should be considered as not individually negotiated. At the moment, personalisation of terms occurs mostly without consumers' knowledge, not to mention they are not given a chance to impact the content of these terms. Even when DSPs are obliged to disclose the use of automated decision-making mechanisms or if, following the BGH's decision, DSPs have a duty to

[74] Ibid, paragraphs 58 and 86.

[75] Judgment of 9 July 2020, *Ibercaja Banco SA*, C-452/18, EU:C:2020:536, paragraphs 33-38.

provide a choice to consumers in what services, under what terms, they choose, this will not signify that contractual terms have been individually negotiated.

We **recommend**, however, that in order to avoid any legal uncertainty as to this matter, the UCTD framework clarifies that personalised terms still fall within the scope of the unfairness test of the UCTD.

2.8. Reputational terms

2.8.1. Rewarding positive reviews

There is a clear business interest for a DSP to reward positive reviews and try to prevent consumers from writing negative reviews.[76] The UK's Competition and Market Authority (CMA) estimated that ca £23 billion a year of consumer spending is influenced by online customer reviews.[77] UK's consumer organisation " Which? " has further found out that consumers could be more than twice as likely to buy a poor-quality product that had been supported by fake reviews (Lester, 2020). Recital 47 MD rightly then indicates that consumers increasingly rely on consumer reviews and endorsements when they make purchasing decisions. In order to protect consumers from fake reviews, the MD has introduced as per se a forbidden commercial practice the case where a trader submits or commissions another legal or natural person to submit false consumer reviews or endorsements, or misrepresents consumer reviews or social endorsements, in order to promote products.[78] National consumer and market authorities have already been policing DSPs as to fake reviews found on their website. For example, Facebook and eBay pledged to the CMA to better identify, investigate and respond to fake and misleading reviews on their platforms.[79]

Offering a reward for a positive review could possibly be seen as commissioning a consumer to submit a false review and therefore might qualify as a misleading commercial practice. Often, online platforms would actually prohibit DSPs and online traders active on their platform from incentivised reviews in their policies. For example, this was the case with Amazon's Choice service, although many violations of this policy have been discovered (Simmonds, 2020).

It is clear that offering a reward for a positive review may invite consumers to evaluate a DSP or a digital service in a less than truthful manner. If, therefore, a contract is concluded between a DSP and a consumer, which terms specify that consumers will be rewarded for providing positive reviews of the digital services or of the DSP in the future, we could question whether such terms could be considered as unfair. Moreover, separate contracts may be concluded specifically to commission fake reviews and to recruit people to write such, e.g. after a web sweep CMA found ca 100 eBay listings offering fake reviews for sale.[80] The difficulty with applying the framework of the UCTD lies here in the possible harm being caused to other consumers, rather than the contractual partner of the DSP. Consequently, we

[76] See also previous briefing for the EP, 'Online consumer reviews. The case of misleading or fake reviews' (October 2015) <https://www.eesc.europa.eu/resources/docs/online-consumer-reviews---the-case-of-misleading-or-fake-reviews.pdf> accessed 4 December 2020.

[77] <https://campaigns.which.co.uk/fake-reviews/> accessed 1 December 2020.

[78] See item 23c in Annex I UCPD.

[79] CMA, 'Facebook and eBay pledge to combat trading in fake reviews' (8 January 2020) <https://www.gov.uk/government/news/facebook-and-ebay-pledge-to-combat-trading-in-fake-reviews> accessed 1 December 2020. Further investigation is pending: CMA, 'CMA investigates misleading online reviews' (22 May 2020) <https://www.gov.uk/government/news/cma-investigates-misleading-online-reviews> accessed 1 December 2020.

[80] CMA, 'CMA expects Facebook and eBay to tackle sale of fake reviews' (21 June 2019) <https://www.gov.uk/government/news/cma-expects-facebook-and-ebay-to-tackle-sale-of-fake-reviews> accessed 1 December 2020.

think that the framework of the UCPD is better suited to tackle such commercial practices rather than the UCTD framework.

2.8.2. Prohibiting negative reviews

This is different with regard to terms prohibiting negative reviews. Such terms do not only have an adverse effect on the reliability of online reviews, they also impair a consumer's freedom of right of expression and information as guaranteed under Article 11 EU Charter of Fundamental Rights. A notorious example is a term in the terms and conditions of a UK hotel, on the basis of which it fined a couple £100 for leaving a bad review on the travel review website Trip Advisor.[81]

Such terms clearly only have disadvantages for consumers, and there is no doubt that a trader, dealing fairly and equitably with the consumer, could not reasonably assume that the consumer would have agreed to such a term in individual contract negotiations.[82] For this reason, **we recommend** that terms prohibiting negative reviews are blacklisted.

2.9. Terms contradicting GDPR principles and rights

In the paragraphs below we briefly introduce selected GDPR data processing principles and a few rights of data users that the GDPR introduces. We outline what actions they require from DSPs. If DSPs do not comply with such obligations, they could find themselves in breach of the GDPR. However, we also **recommend** that any terms that would result in the breach of these principles or rights, should also be considered as unfair within the meaning of the UCTD (Helberger, Zuiderveen Borgesius, and Reyna, 2017, p. 1451). This may either provide consumers with additional remedies, e.g. an option to withhold performance, not allow DSPs to rely on their liability exclusion or limitation clauses, or (as is discussed in paragraph 4.3, at least for cross-border contracts) allow courts to terminate the contract if this is more advantageous to the consumer than merely leaving the term contradicting the GDPR out of consideration.

2.9.1. Data minimisation principle

Article 5(1)(c) GDPR provides that personal data shall be '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'. This principle aims to minimise the personal data collection by DSPs. As the Information Commissioner's Office (ICO) has explained, DSPs should ensure that they process the minimum amount of personal data required to fulfil their purpose.[83] Moreover, this principle requires data controllers to periodically review the personal data they hold and delete anything that is no longer relevant (see also paragraph 2.9.3).

If DSPs draft terms allowing them to go beyond the data minimisation principle,[84] they will be clearly in breach of the GDPR. However, we may also wonder whether such terms could not be considered unfair by the UCTD. For example, if consumers are asked to agree to terms allowing DSPs to collect more data than what they need for the provision of the service, that could be seen as introducing a significant imbalance in the contractual rights and obligations of the parties. After all, consumers will not be remunerated for the data they provide in excess of the cost of the service they acquire (Helberger, Zuiderveen Borgesius and Reyna, 2017, p. 1445). Again, we should reiterate here that the personal data may serve as counter-performance and DSPs may determine the scope of the personal

[81] See <https://www.bbc.co.uk/news/technology-30100973> accessed 23 November 2020.

[82] Judgment of 14 March 2013, *Aziz*, case C-415/11, EU:C:2013:164, paragraph 69.

[83] See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/> accessed 4 December 2020.

[84] For examples of DSPs asking for more data than the data minimisation principle allows see: Forbrukerrådet, 2016a, pp. 33-36.

data that they will require to provide their services, just like they could determine the amount of the monetary price for them. However, where this is not the case, the data minimisation principle may be infringed. The Norwegian Consumer Council noted that e.g. fitness wristbands collected more data than what was necessary to provide the service (Forbrukerrådet, 2016b).

It needs to be mentioned that, generally, the unfairness test excludes from its scope core terms, which notion encompasses also testing the adequacy of the price and remuneration against the services supplied in exchange. It is left to the market to determine what price is just for the provision of given services. If a term infringing the data minimisation principle is perceived as unfair, this assessment would need to occur, therefore, on the basis of that term limiting the consumers' right to have their data minimised, following the GDPR or the lack of transparency of such a term.[85]

Previously, for example the French Tribunal de Grande Instance of Paris decided that terms of Google+ service were unfair when they alluded to the personal data being collected for the better provision of the service, even though Google+ collected the data also for commercial purposes (Que Choisir, 2019).

If terms infringing data minimisation principle are considered unfair, then consumers, aside having the right from the GDPR to ask for the erasure of any data provided beyond the minimisation principle, pursuant to Article 17(1)(d) GDPR, could also refuse to provide such data. After all, if the term allowing DSPs for such data collection is unfair, it is not binding, and therefore consumers do not need to comply with it. Despite consumers not providing such data, DSPs would still remain obliged to perform their contractual obligations, i.e. provide digital services to the consumer. Unless, of course, the contract could not survive the removal of the term, i.e. the term allowing for the data collection would be a core contract term, non-transparently drafted, and as a result of its unfairness the whole contract could be voided. Following the UCTD framework, consumers would then retain the choice of objecting to the annulment of their contract, in order to keep access to the digital services. However, as the data we mention here is the data collected in excess of what was necessary to provide the digital service, whether from a functional or a commercial point of view, it is highly unlikely that the necessity of its provision could be seen as a core contractual term. The right to withhold performance in such cases, if facilitated from a technological point of view, i.e. by consumers installing apps blocking the additional data collection, could possibly help consumers where the procedures about the infringement of data protection rules take a long time.[86]

2.9.2. Accuracy principle – access, rectification, erasure

Article 5(1)(d) GDPR stipulates that personal data shall be accurate and, where necessary, kept up to date. This means further that the inaccurate data should be able to be erased or rectified without delay. The ICO further emphasised that the data should not only be accurate but also not misleading and that data controllers should have appropriate processes in place to ensure the accuracy of the data.[87] Consumers may themselves ask DSPs to correct their data, on the basis of their right to rectification, pursuant to Article 16 GDPR. However, if DSPs use their own resources to compile personal data about consumers, they need to do this diligently from the outset. Further, if they obtain such data from other

[85] Unless the personal data is not perceived as a price and a clause referring to its collection would not be seen as a core term, see Helberger, Zuiderveen Borgesius, and Reyna, 2017, pp. 1450-51.

[86] For example, two years ago complaints have been filed against Google for collecting users' location data and the use of dark patterns to do so, which complaints are still far from being resolved, see BEUC, 'Commercial surveillance by Google. Long delay in GDPR complaints' (26 November 2020) <https://www.beuc.eu/press-media/news-events/commercial-surveillance-google-long-delay-gdpr-complaints> accessed 1 December 2020.

[87] See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/> accessed 1 December 2020.

parties, they should note the source of the information and still take reasonable steps to ensure the accuracy of the acquired information.

For example, the French Tribunal de Grande Instance of Paris found that terms of Google+ service allowed Google+ to keep a log of old data that users sought to rectify, which was deemed to infringe data protection principles and such terms were declared unfair (Leone, 2019).

We would **recommend** considering as unfair a term in which a DSP claims that they bear no liability for the accuracy of the personal data. This would infringe the above-mentioned provisions and create an impression with consumers that they have no right to demand from DSPs that they ensure the accuracy of their personal data. This right could be explicitly linked to Article 1(b) of the Annex to the UCTD, which presumes unfairness of clauses inappropriately excluding or limiting consumers' rights against DSPs for the non-performance of their contractual obligations.

2.9.3. Storage limitation principle

Article 5(1)(e) GDPR requires data controllers to limit the amount of time during which they store personal data, generally, to the timeframe necessary to achieve the purposes for which the data is being processed. Whilst the data minimisation principle focuses on the amount of the collected data, this principle addresses the time frame during which it is processed. This time frame should be set up carefully, as consumers have the right to have their data erased, when it is no longer necessary.[88]

DSPs as data controllers need to outline in their terms and conditions, in which we count privacy policies (see paragraph 1.2.2), their standard data retention periods. Such terms should clearly inform consumers about the timeframe for which their data is being collected. If the terms are vague, they do not specify the limit to the data storage or they do not oblige DSPs to review and erase no longer needed data, such terms could not only infringe the GDPR, but also be considered as unfair. As the Norwegian Consumer Council has found e.g. producers of fitness wristbands do not state for how long they will retain user data (Forbrukerrådet, 2016b).

As a term, which unclearly, inaccurately or in a misleading way limits data storage would then be non-binding, a gap would be created in the contract upon the recognition of that term's unfairness. Therefore, we would **recommend** the introduction of default rules regarding the limitation of storage of personal data, in order to protect consumers from having their data collected indefinitely. For example, DSPs could be obliged to remove the collected data within a reasonable time from the moment such data becomes unnecessary for the provision of their services. The DSPs should also comply with Article 16 DCD in this respect (see paragraph 2.4.2). Such default rules could be added to the Digital Services Act.

A practical problem that may arise here is that many users will never actually delete their accounts with DSPs when they stop using their services, instead opting in for not using the service anymore or simply uninstalling the app from their devices (Forbrukerrådet, 2016a, pp. 51-53). These practices do not delete the users' account with the DSP and, therefore, do not provide a signal to the DSP to stop using the personal data of this user. Therefore, we **recommend** considering as unfair such terms of DSPs that allow for an open-ended timespan for the storage of consumers' data. Each DSPs should introduce a retention period for their data storage and could add a notification to their users, when that period was ending, allowing them to opt in for preserving their data with the DSPs for an additional period of time.

[88] See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/> accessed 1 December 2020.

2.9.4. Integrity and confidentiality principle

Article 5(1)(f) GDPR intends to assure the personal data's security, by obliging data controllers to take measures to that effect by means of '*appropriate technical and organisational measures*'.[89] This provision obliges DSPs to investigate whether they have taken reasonable steps to ensure the protection of the personal data, e.g. through encryption or pseudonymisation. However, empirical research has shown that DSPs struggle to properly anonymise the personal data of their users (Forbrukerrådet, 2016a, pp. 47-49) and to ensure that e.g. connected goods, such as toys (Forbrukerrådet, 2016c) or kids' smartwatches (Forbrukerrådet, 2017), are secure from third parties connecting to them and accessing their data (BEUC, 2019). Moreover, they should establish security protocols in the case of any data breaches, that would allow them to minimise their damage and restore access and availability to personal data. They should also clearly explain who they will be sharing the personal data of consumers with, whilst often in practice DSPs simply reserve the right to share the data with third parties (Forbrukerrådet, 2016b).

Here, again, we would **recommend** to consider as unfair such terms of the DSPs' privacy policies that would limit their liability for any breach of data security (see paragraph 2.2.5). DSPs should not give an impression to consumers that they would not be liable if such a breach results from their negligence and their infringements of the GDPR principles.

2.9.5. Right to data portability

Article 20 GDPR provides consumers with the right to data portability, where consumers shared their data based on consent to data processing or where collection of data was necessary for the performance of the service. Both of these grounds would likely be the most common justifications used by DSPs for consumers' data collection. The right to data portability enables consumers to request from DSPs the provision of their data that they have shared with the given DSP. This data has then to be issued to consumers in a '*structured, commonly used and machine-readable format*'. Consumers should be facilitated in transferring this data to another data controller (Forbrukerrådet, 2016a, p. 55). A similar right exists in the case the consumer terminates the contract for the lack of conformity of the digital service or where the digital service is changed by the DSP for other reasons than to keep the digital service in conformity with the contract, and that change has a (more-than-minor) negative impact on the consumer's access to or use of the digital service (Articles 14(1), 16(4) and 19(2) DCD).

The right to data portability allows consumers to reuse their data across different services, as the usability of data should not be affected by the transfer between different DSPs.[90] There is a clear advantage for consumers in this right, as having access to an effortless transfer of data between services should facilitate and encourage switching between DSPs, allowing consumers to obtain the best deal. Generally, consumers should be able to obtain and transfer their data without having to pay any fees and within a reasonable time, usually within one month from issuing the request.

If DSPs mislead or deter consumers from the use of their right to data portability in their privacy policies, we would **recommend** to consider such clauses unfair. This could happen, e.g. if a term in privacy policies of a DSP: introduced fees for transferring data from that DSP to another; stated that it was impossible to transfer personal data of consumers, without providing them with reasons why this would be the case and/or without advising them of their right to complain against this decision; or

[89] See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/> accessed 1 December 2020.

[90] See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/> accessed 4 December 2020.

stated that the data will be provided to consumers in a format that is not widely-used, and, therefore, would not be easily readable for another DSP.

2.9.6. Right to withdraw consent

Article 7(3) GDPR specifies that data subjects have the right to easily withdraw their consent at any time and they should be informed about this right. The fact that consumers should be facilitated to withdraw from the obligation to provide their personal data at any time they choose means that they should be able to do this of their own initiative, without being prompted to do this by DSPs. Consequently, DSPs should provide an easy way, a 'one-step process', for withdrawing the consent on their websites, where such consent was given in the first place.[91] There should not be any penalty attached to consumers deciding to withdraw their consent, as it may be freely given and freely taken away.

It needs to be mentioned here that DSPs may require collecting and processing of personal data in order to be able to actually provide consumers with their digital services, either because the functionality of the service requires this or due to the use of the data as payment. However, if that is the case, they should acquire consumers' personal data on a legal basis other than the consent to data processing, as they may not object to the withdrawal of the consumers' consent on the grounds of trying to preserve the contractual relationship. Consequently, choosing a different ground to justify the data collection would protect both DSPs and consumers from a situation, in which consumers would withdraw their consent.

We **recommend** that any terms of DSPs that deny consumers the right to withdraw their consent or hinder the use of such a right, e.g. by introducing a complex consent withdrawal procedure or introducing a penalty fee for the withdrawal, are considered unfair. It will be less straightforward to assess terms as unfair where they link the withdrawal of the consumers' consent with the suspension or termination of the provision of digital services. If the personal data was perceived as payment for the provision of digital services, then from the moment that DSPs are to stop processing the data, there is no counter-performance of consumers for an access to such services (see further paragraph 2.4.1).

2.10. Terms on conflict resolution

2.10.1. Alternative dispute resolution mechanisms

DSP's terms and conditions in many ways aim at hindering consumers from taking legal action or exercising a legal remedy. Such terms all fall within the scope of Article 1(q) of the Annex to the UCTD. The first form in which such terms appear, is that of an arbitration clause often requiring the consumer to accept that any dispute or claim is subject to binding arbitration. For instance, the Terms of Service of Epic Games,[92] the DSP offering the online game Fortnite, provide as follows:

> *'2. You and Epic agree to resolve disputes between us in individual arbitration (not in court). We believe the alternative dispute-resolution process of arbitration will resolve any dispute fairly and more quickly and efficiently than formal court litigation. We explain the process in detail below, but we've put this up front (and in caps) because it's important:*
>
> *THESE TERMS CONTAINS A BINDING, INDIVIDUAL ARBITRATION AND CLASS-ACTION WAIVER PROVISION. IF YOU ACCEPT THESE TERMS, YOU AND EPIC AGREE TO RESOLVE DISPUTES IN BINDING, INDIVIDUAL ARBITRATION AND GIVE UP THE RIGHT TO GO TO COURT INDIVIDUALLY OR AS PART OF*

[91] See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/#how6> accessed 4 December 2020.

[92] <https://www.epicgames.com/site/en-US/tos> accessed 23 November 2020.

A CLASS ACTION, AND EPIC AGREES TO PAY YOUR ARBITRATION COSTS FOR ALL DISPUTES OF UP TO $10,000 THAT ARE MADE IN GOOD FAITH (SEE BELOW).'

The Terms of Service thus clearly indicate that consumers give up the right to go to court individually or as part of a class action, suggesting that collective action is not possible either. Since such a term withholds the consumer from the right to go to court, it impairs the consumer's rights under Article 47 EU Charter of Fundamental Rights. Given the fact that the average consumer is not expected to possess legal knowledge[93] and is therefore not capable of sufficiently understanding the disclaimer at the end of the following clause, we believe the same is true for the Amazon Prime Video Terms of Use,[94] which under 6 (Additional terms) contain the following clause:

'*g. Disputes/Binding Arbitration/Conditions of Use. Any dispute or claim arising from or relating to this Agreement or the Service is subject to the governing law, disclaimer of warranties and limitation of liability, binding arbitration and class action waiver (if applicable), and all other terms in the Amazon Conditions of Use of your Video Marketplace (noted here). You agree to those terms by using the Service. YOU MAY ALSO BE ENTITLED TO CERTAIN CONSUMER PROTECTION RIGHTS UNDER THE LAWS OF YOUR LOCAL JURISDICTION.*'

This latter clause is non-transparent and should therefore also be held unfair. For this reason, **we recommend** that clauses requiring consumers to submit claims to arbitration or to accept being submitted to arbitration or suggesting that consumers are required to do so, are to be declared unfair under all circumstances and thus are blacklisted.

2.10.2. Forum choice clauses

Whereas arbitration clauses prevent consumers from going to any court, forum choice clauses (or jurisdiction clauses) may deprive the consumer from their right to go to a court in the country where they live. For instance, in its Microsoft Customer Agreement, Microsoft indicates that if it brings an action against the customer they will do so where the customer (whether that is a business or a consumer)[95] has their headquarters (sic!). However, if a European customer brings an action against Microsoft they have to bring the action in the State of Washington (USA) or, if the action is exclusively against Microsoft or any Microsoft Affiliate located in Europe, in Ireland.[96] The jurisdiction clause in Epic Games' Terms of Service requires the consumer in all cases to go to court in the State of North Carolina (USA).[97]

For contracts that DSPs conclude with a consumer, these provisions derogate to the detriment of the consumer from the jurisdiction provisions of the Brussels I Regulation (recast), which allow the consumer to bring the claim before a court in the country where they are domiciled.[98] Importantly, this derogation occurs before a dispute has arisen between the parties, which means that consumers may

[93] Judgment of 28 July 2016, *VKI/Amazon EU*, case C-191/15, EU:C:2016:612, paragraphs 66-71.

[94] These terms are applicable in the UK and in all EU Member States except Germany and Austria <https://www.primevideo.com/help/ref=atv_hp_nd_cnt?nodeId=202095490> accessed 23 November 2020 (last updated on 15 September 2020).

[95] The Microsoft Customer Agreement <https://www.microsoft.com/licensing/docs/customeragreement. accessed 24 November 2020 (last updated 18 October 2019), refers to the possibility that the customer is a consumer in two provisions of the Supplemental Individual User Purchase Terms that apply whenever the customer is an individual.

[96] ibid, section Miscellaneous, under (l); this provision applied even when we indicated that we lived elsewhere in the EU.

[97] See the Epic Games' Terms of Service, section Governing Law and Jurisdiction <https://www.epicgames.com/site/en-US/tos> accessed 1 December 2020.

[98] See Article 18(1) Brussels I Regulation (recast).

not be aware of the significance of this term. **We recommend**, therefore, to explicitly declare such terms as being unfair.

2.10.3. Applicable law clauses

Another way to potentially deprive consumers from their legal rights is to introduce an applicable law clause. Even though such a clause cannot deprive the consumer from the protection offered by the mandatory law of the otherwise applicable law of the country where they live,[99] a consumer – who is not expected to have legal knowledge[100] – may be misled by such a clause in believing their legal position is governed by a law they are not familiar with, and for that reason refrain from taking legal action. Notwithstanding the fact that the CJEU already declared such terms to be lacking transparency and unfair in 2016,[101] such clauses still are frequent in contracts concluded with major DSPs. For instance, in the Microsoft Customer Agreement, Irish law is indicated as the applicable law,[102] and Epic Games' Terms of Service indicate that the contract is governed by North Carolina law.[103] Similarly, Dropbox' Terms of Service[104] indicate that California law applies, but these Terms of Service recognise that

> '*some countries (including those in the European Union) have laws that require agreements to be governed by the local laws of the consumer's country. This paragraph doesn't override those laws.*'

In our view, such a provision still does not make clear to an average consumer that their particular contract indeed is governed by the law of the country in which they live. We therefore argue that such a provision also sheds confusion as to the protection offered by the consumer's national law and should be considered unfair. In order to prevent such confusion, **we recommend** that applicable law clauses that do not explicitly indicate that the consumer may always rely on the mandatory consumer protection laws of the country where they live, are to be blacklisted.

2.11. Terms on copyright

2.11.1. Gratuitous license for user-generated content

Some DSPs require the consumer to grant them a license to use the content the consumer has generated on their platform or by using their service. Where this user-generated content is needed by the DSP in order to provide the digital service, of course such license is not problematic. However, where the DSP also makes commercial use of the user-generated content and requires the consumer to give them a gratuitous license, they essentially require the consumer to agree to sign away their intellectual property rights for commercial purposes.

For example, in 2015 and 2016 Facebook stated in its clause 2.1 of its Statement of Rights and Responsibilities:

> '*2. Sharing Your Content and Information*
>
> *You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:*

[99] See Article 6(2) Rome I Regulation (Regulation (EC) 593/2008, *OJ* 2008, L 177/6).

[100] Judgment of 28 July 2016, *VKI/Amazon EU*, case C-191/15, EU:C:2016:612, paragraphs 66-71.

[101] ibid.

[102] See the Microsoft Customer Agreement (fn 89), section Miscellaneous, under (k).

[103] See the Epic Games' Terms of Service (fn 91).

[104] <https://www.dropbox.com/terms2018?view_en> accessed 2 December 2020.

1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.'

This clause was subjected to an unfairness test by the Paris Tribunal,[105] which considered the term unclear and confusing, as it did not specify the scope of the licence nor did it allow consumers to terminate the licence with the effect that the user-generated content would have been removed, as well (Pavis, 2019).[106]

Since these provisions are usually hidden away deep in the terms and conditions, and are not presented in a clear and unambiguous manner, consumers typically do not realise that they pay for the digital service not only in money or by providing personal data, but also by offering such a gratuitous license. We agree with the French court that such a provision disturbs the balance between the parties' rights and obligations under the contract in such a manner that the DSP, dealing fairly and equitably with the consumer, cannot reasonably believe that the consumer – if they would realise which negative economic consequences follow for them from the term – would agree to the incorporation of the term in individual contract negotiations.[107] On the other hand, an individual consumer may very well accept the term in case they have been properly informed of the existence and meaning of the term at the moment of conclusion of the contract if in their opinion the advantages they receive under the contract outweigh the totality of obligations they undertake under that contract. **We recommend** that such terms are placed on the grey list, which means they will be presumed to be unfair unless the DSP proves that they have been brought specifically to the consumer's attention at the moment of conclusion of the contract and have been individually, separately and explicitly accepted by the consumer.

2.11.2. Gratuitous license for exploitation of personal data

Similar to clauses awarding a gratuitous license to the DSP for user-generated content, clauses granting the DSP a gratuitous license for the exploitation of the personal data allow the DSP to commercialise data coming from the consumer. As the supply of personal data may, in some respects, be seen as the consumer's counter-performance in case where the consumer does not pay a price in money, such clauses need not be unfair.

This is different, however, where the clause is not brought specifically to the consumer's attention in an intelligible and easily accessible form, using clear and plain language, as in such case the consumer's consent is not given in accordance with Article 7(2) GDPR and, according to that provision, is not binding. Since Article 7(2) GDPR already provides the same sanction as Article 3(1) UCTD does, there is no need to specifically add a provision to the Annex of the UCTD regarding this matter, but **we recommend** that a recital is added in the preamble to the UCTD that where contractual clauses pertain to the supply of personal data, both the provisions of the UCTD and those of the GDPR apply in a complementary manner.

[105] TGI de Paris judgment of 9 April 2019, <https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-9-avril-2019/>.

[106] Similar evaluation occurred in cases against Google: TGI de Paris judgment of 12 February 2019, <https://www.legalis.net/jurisprudences/tgi-de-paris-jugement-du-12-fevrier-2019/> and Twitter: TGI de Paris judgment of 7 August 2018 <https://entreprises.claisse-associes.com/wp-content/uploads/2018/08/TGI-Paris-7-ao%C3%BBt-2018-UFC-Twitter.pdf>.

[107] Judgment of 14 March 2013, *Aziz*, case C-415/11, EU:C:2013:164, paragraph 69.

3. TRANSPARENCY ONLINE

Article 5 UCTD requires terms and conditions, including those provided online, to be drafted in "plain, intelligible language". Further, Article 4(2) UCTD excludes from testing for unfairness such core terms of the contract that have been provided to consumers in "plain intelligible language".

The UCTD does not specify, however, what sanctions should follow when traders and service providers breach the principle of transparency (Loos, 2015, pp. 184-189). Moreover, the assessment whether terms have actually been provided in a transparent manner to consumers may differ between the Member States and even within the Member States (Junuzović, 2018; Luzak, 2020a; Seizov and Wulf, 2020). Further guidelines on the meaning and application of the principle of transparency are missing in EU consumer law. These general problems with the current application of the UCTD apply also to the provision of digital services. This paragraph will focus, however, on issues that tend to be more prevalent in the provision of digital services.

The first issue with the transparent provision of terms and conditions online relates to the lack of clear delineation of what information given to consumers actually constitutes such terms and conditions (see also paragraph 1.2.2). For example, DSPs may easily set up different pages on their website, separating information provided to consumers on payment, delivery, etc. and consumers may not know, which, if any, of this information sets out their contractual rights and obligations (Loos and Luzak, 2016, p. 87).[108] Moreover, DSPs may claim that privacy policies are not part of their terms and conditions and, therefore, cannot be tested for unfairness (Loos and Luzak, 2016, pp. 65-67).[109] The discrepancy between the practices of DSPs and their terms and conditions may contribute to the consumers' lack of awareness about their rights and about the responsibilities of DSPs (Ducato and Strowel, 2019, p. 128). To strengthen legal certainty in the relationship between DSPs and consumers, it could be **recommended** to extend the principle of transparency from the UCTD to apply to DSPs providing information as to which of their online disclosures are part of their terms and conditions. Alternatively, this obligation could be added to the CRD or the Digital Services Act.

As the online environment provides additional options for disclosing terms and conditions to consumers than when these are disclosed in more traditional manners, i.e. on a piece of paper or orally, the assessment of their transparency may need to be approached differently, as well (Hogarth and Merry, 2011). The points below outline, therefore, different options of providing information to consumers online and emphasise the issues this might bring about.

3.1. Online design options

3.1.1. Visualisation of information (e.g. icons)

One of the advantages of disclosing information to consumers online rather than offline is the multitude of graphic design options and various multimedia that could be used to make the online terms and conditions more transparent. The importance of visualisation in increasing transparency of consumer information has been already recognised in some European legislation (Recital 58 GDPR), as

[108] See e.g. on Facebook's Data Use Policy consisting of no less than 6 separate documents, which also kept on referring consumers to other sources of information on this policy.

[109] As we have argued before, provided that such policies determine the rights and obligations of the parties they should be perceived as contractual terms.

well as in soft law.[110] Consequently, DSPs have been recommended the use of icons, table-like displays and other graphical elements that could make consumer information more accessible to average consumers. As scholars have noted, however, such recommendations were mainly made in soft law and were, therefore, not binding (Rossi and others, 2019, p. 83).[111] Behavioural research studies provide increasing indications that information provided in a visual way may be more accessible to consumers and prompt their engagement with this information (Alkazemi and Van Stee, 2020, p. 136; Sheng and others, 2020). Therefore, we **recommend** that an update of the UCTD considers including a stronger recommendation for DSPs to use icons and other graphical aids to convey information. This could be added to the Digital Services Act.

3.1.2. Layering of information (e.g. hyperlinks)

Another feature that is typical for the online environment is the option to easily layer information. This can be achieved through the use of hyperlinks, for example. Hyperlinks allow DSPs to provide the main information to consumers in a shorter text. Through hyperlinks they may refer consumers to other web pages containing additional information on particular issues. This practice may allow to avoid the consumers' feeling information overload and being discouraged from reading a long disclosure online. The purpose of layering is then to also enhance learning (Seizov, Wulf and Luzak, 2019, p. 160; Djonov, 2007).

Another example of layering is the use of mouseovers (or mouse hover boxes), which means that additional information may be displayed on the same webpage when a consumer moves the pointer on the screen over a particular trigger area. This could also allow to provide more extensive, additional information, e.g. definitions of more technical words included in the online terms and conditions, to consumers without expanding the main text on the screen (Seizov, Wulf and Luzak, 2019, p. 168). One critique of mouse-overs that comes to mind, however, is that they may be difficult to access on smartphones and other electronic devices with smaller screens. However, contrarily to hyperlinks, they can be activated more easily also by passive consumers (Seizov, Wulf and Luzak, p. 160).

Previously, the CJEU expressed doubts as to the effectiveness of the provision of mandatory information via hyperlinks to consumers, focusing on the passive role that consumers tend to play in relation to the information (Djonov, 2007).[112] Therefore, the assumption was that consumers will not click on the hyperlink and access the information, which would effectively allow DSPs to hide some of the essential information behind a hyperlink. Similarly, the willingness of consumers to use mouseovers could be questioned, which could lead to the perception that information provided through the use of mouseovers was not transparent.

Considering the above-mentioned beneficial effects of the use of hyperlinks on consumers' engagement and attention, it might be worth it to **reconsider** the assessment of the transparency of such online disclosures, which layer the consumer information. For example, the French Tribunal de Grande Instance of Paris found that a practice of Google+ to split its contractual terms and conditions to both 'terms of use' and a 'privacy policy', as well as their use of hyperlinks to layer the text, was transparent (Leone, 2019). However, as mentioned-above, if the layering of information leads to the provision of terms and conditions on different webpages, in various documents, DSPs should clearly outline and identify all of them. The assessment of the structure in which terms and conditions are

[110] See e.g. European Commission, 'DG Justice Guidance document concerning Directive 2011/83/EU' (June 2014) <https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf> 69.

[111] The European legislator advised the use of icons also in Recital 60 GDPR.

[112] Judgment of 5 July 2012, *Content Services*, C-49/11, EU:2012:419, paragraph 51.

provided to consumers should be as important in the evaluation of their transparency as the language used to express them (Ducato and Strowel, 2019, pp. 138-146).

3.2. Certification and trustmarks

Another way to enhance the use of fair and equitable terms and conditions is to make available terms and conditions that have been scrutinized before they were first used by the trader. An example is the praxis in the Netherlands, where under the umbrella of the SER[113] for many branches of industry consultations take place between trade organizations and consumer organizations about the terms and conditions that are applied by traders in their contracts with consumers. Where these organizations reach an agreement, the resulting 'two-sided' terms and conditions offer a more or less balanced set of terms. A part of the agreement is that the consumer organizations that have taken part in the negotiations lose their collective action rights as regards the agreed terms[114] and that the trade organizations accept the establishment of an alternative dispute resolution (ADR) scheme, which resorts under *De Geschillencommissie,* an officially recognised ADR-entity. Consumers may take it that the terms in the agreed set of terms and conditions by and large indeed offer a balanced set of terms. The agreement of consumer organizations is taken into account by courts when ascertaining individual terms as it may indicate that an otherwise potentially unfair term may be compensated by an extra advantageous other clause in the set of contract terms.[115] For individual consumers *and* traders, the fact that consumer organizations have agreed to the text of these terms and conditions may provide trust in the fairness of the terms, and for traders some degree of legal certainty as to their validity.

A further step is that a set of terms and conditions – whether issued by a trader or negotiated between trade and consumer organizations – are certified by a national consumer authority or another independent body. In practice this boils down to an *ex ante* test of the unfairness of the set of terms. In case of a certification by a national consumer authority the terms may potentially even escape the unfairness control altogether in case the use of terms is obligatory for the trader as under Article 1(2) UCTD, contractual terms which reflect *mandatory* regulatory provisions are not subject to the provisions of the UCTD. In case of certification by a private entity, the terms in any case remain subject to the unfairness test. However, the *ex ante* control may then be combined with the creation of a trustmark, which can be used on the trader's website. An example is the Ecommerce Europe Trustmark, which intends to show consumers (also when concluding a cross-border contract) that the trader complies with European consumer law, including also unfair terms legislation.[116] The use of the trustmark may then signal to consumers that the concerned trader acts fairly towards them.

We recommend that the European Commission be empowered to further stimulate the development of 'two-sided' terms and the development of *ex ante* testing of terms and conditions and of trustmarks.

3.3. Language of disclosure

In *Kásler*, the CJEU held that in order to comply with the transparency requirement in Article 5 UCTD, the consumer must be able to ascertain the economic consequences that result from a term.[117]

[113] The Social and Economic Council of the Netherlands (SER) is an advisory body consisting of representatives from the industry, trade unions and independent experts (Crown-appointed members). Within the SER, these representatives and experts work together to reach agreement on key social and economic issues. See <https://www.ser.nl/en/SER/About-the-SER/What-is-the-SER> accessed 2 December 2020.

[114] See Article 6:240(5) Dutch Civil Code.

[115] See Dutch Supreme Court 3 February 2012, ECLI:NL:HR:2012:BT6947. See in a similar vein also German Federal Supreme Court (BGH) 4 May 1995, *Neue Juristische Wochenschrift* 1995, 2224.

[116] <https://www.ecommerce-europe.eu/ecommerce-europe-trustmark/> accessed 2 December 2020.

[117] Judgment of 30 April 2014, *Kásler*, case C-26/13, EU:C:2014:282, paragraph 73.

According to the CJEU, it is on the basis of that evaluation that the consumer decides whether they wish to be contractually bound by agreeing to the terms previously drawn up by the trader.[118] To that extent, it is not sufficient that the term is formally and grammatically intelligible. Instead, the transparency requirement is to be interpreted broadly, the CJEU emphasises.[119] Where a term is not transparent, a national court needs to consider this when it assesses the term's unfairness under Article 3 (1) UCTD.[120] The transparency requirement is therefore an important element in the protection of the consumer against unfair terms.

However, the UCTD does not pose specific language requirements. This implies that it is up to the trader to determine the language in which they draft their terms and conditions. Typically, they will draft these terms in their own language. However, since DSPs often operate throughout the European Union, this brings along the risk that a consumer with whom they contract will not understand the terms and conditions because they do not master the language in which they have been drafted. If that is the case, the consumer cannot ascertain the economic consequences of the terms and therefore cannot base their contracting decision thereupon. As this is foreseeable for any DSP that offers their digital services to consumers in another country, in our view, such a breach of transparency should be sanctioned by unfairness of these terms. For this reason, **we recommend** to clarify – either in the preamble or in Article 5 UCTD itself – that where consumers are targeted who are domiciled in another country than where the trader has their seat of business, terms that are not provided in one or more official languages of the country where the consumer lives are deemed to be unfair.

3.4. Vulnerable consumers' needs

An additional question that arises in testing the transparency of terms and conditions drafted by DSPs relates to the benchmark consumer, who is the intended reader of such terms and conditions. The UCTD does not specify who the benchmark consumer is. Following the CJEU's case law,[121] the unfairness test seems to assess whether terms and conditions are transparent to an *average* consumer, that is a reasonably well-informed, observant and circumspect consumer.[122] Any revision of the UCTD should **consider** adding an explicit mention of an appropriate benchmark for consumer protection (Luzak, 2020b).

With this in mind, it should be evaluated whether consumers of digital services are indeed effectively protected against unfair terms, if the benchmark is set at the level of an average consumer, at least considering how this benchmark has been interpreted so far. The continued evidence of the use of big data thanks to the application of complex algorithms by DSPs, especially belonging to Big Five companies, raises issues related to the application of enhanced persuasive practices by DSPs (Kaptein and others, 2015; Mik, 2016; Susser, Roessler and Nissenbaum, 2019; Jabłonowska and others, 2018). Certain national consumer and market authorities, as well as courts, have already expressed their concern with various personalisation practices, which online consumers may not have a choice in

[118] Judgment of 23 April 2015, *Van Hove*, case C-96/14, EU:C:2015:262, paragraph 41.

[119] ibid; judgment of 28 July 2016, *VKI/Amazon EU*, case C-191/15, EU:C:2016:612, paragraphs 65 and 68.

[120] Judgment of 23 April 2015, *Van Hove*, case C-96/14, EU:C:2015:262, paragraph 27; judgment of 28 July 2016, *VKI/Amazon EU*, case C-191/15, EU:C:2016:612, paragraphs 65 and 68.

[121] Judgment of 30 April 2014, *Kásler,* C-26/13, EU:C:2014:282, paragraph 74; judgment of 26 February 2015, *Matei,* C-143/13, EU:C:2015:127, paragraph 75; judgment of 23 April 2015, *Van Hove,* C-96/14, EU:C:2015:262, paragraph 47; judgment of 9 July 2015, *Bucura,* C-348/14, EU:C:2015:447, paragraph 66; judgment of 20 September 2017, *Andriciuc and Others,* C-186/16, EU:C:2017:703, paragraph 51; judgment of 20 September 2018, *OTP Bank and OTP Faktoring*, C-51/17, EU:C:2018:750, paragraph 78; order of 22 February 2018, *ERSTE Bank Hungary*, C-126/17, EU:C:2018:107, paragraph 35; judgment of 3 March 2020, *Gómez del Moral Guasch,* C-125/18, EU:C:2020:138, paragraph 56; judgment of 9 July 2020, *Ibercaja* Banco, C-452/18, EU:C:2020:536, paragraphs 46 and 55.

[122] See judgment of 16 July 1998, *Gut Springenheide*, C-210/96, EU:C:1998:369, paragraph 31. See also Recital 18 UCPD.

accepting (Podszun, 2019; Haucap, 2019).[123] Consequently, this may lead to consumers finding themselves in a more imbalanced contractual position than ever before and further exacerbate their vulnerability. This vulnerability would also have a structural and external dimension, rather than focus on specific internal characteristics of individual consumers that could lead to the recognition of consumer vulnerability at the moment, pursuant to Article 5(3) UCPD (Helberger and others, 2020). It could create or reinforce digital inequality, e.g. by following gender-stereotypes (Bol and others, 2020, pp. 2001, 2010-12).

Although empirical studies showed that consumer vulnerability may be higher in energy and finance sectors than in the online sector, generally, consumer vulnerability remains a key concern.[124] Therefore, it should be **considered** whether the assessment of transparency of standard online terms and conditions should not use as a benchmark a vulnerable rather than an average consumer. This may require, as the German Federal Supreme Court seems to think, drawing explicit attention of consumers to the fact that DSPs will collect and process consumers' personal data shared not only directly with the DSP but also off-site (e.g. on other online websites, to which the DSP can track consumers' activity).[125] The principle of transparency would then require obtaining specific and explicit, as well as free, consent of consumers to such practices. The free aspect of such a consent requires DSPs to enable consumer access to their services also without accepting such far-reaching personalisation practices.

[123] BGH decision of 23 June 2020, KVR 69/19.

[124] European Commission, 'Consumer vulnerability across key markets in the European Union. Final report' (report by London Economics, VVA Consulting and Ipsos Mori consortium of January 2016) <https://ec.europa.eu/info/sites/info/files/consumers-approved-report_en.pdf>; European Commission, 'Understanding consumer vulnerability in the EU's key markets' (factsheet, February 2016) <https://ec.europa.eu/info/sites/info/files/consumer-vulnerability-factsheet_en.pdf>.

[125] BGH decision of 23 June 2020, KVR 69/19.

4. SANCTIONS FOR UNFAIR TERMS OF DIGITAL SERVICE PROVIDERS

4.1. Non-binding effect of terms

As explained above, section 1.1.4, Article 6(1) UCTD provides that an unfair term may not bind the consumer. However, since the unfairness of a term must be ascertained taking into account all circumstances of the case, the outcome of the unfairness test is to a large extent uncertain for both the DSP and the consumer. This is further complicated by the fact that the yardstick to determine the possible unfairness of a term is the extent to which it derogates, to the detriment of the consumer, from the otherwise applicable provision of national contract law.[126] Since the national contract laws of the Member States differ significantly in all areas where European law has not fully and exhaustively harmonized the relevant legal provisions, the outcome of the unfairness test may also differ from one Member State to the next.

This implies that even for a DSP whose terms have been agreed upon with a consumer organization in one Member State or tested *ex ante* by a national consumer authority or another independent body, and have been tested *ex post* in a court of that Member State, it is uncertain whether a term is allowed or not. In this respect, it would be advisable if at European level, in any case for DSPs that offer their digital services in more than one Member State, a binding list of unfair terms and a binding list of possibly unfair terms would be created.

The first list would be a black list with terms that would be forbidden in all Member States. The second list could be called a grey list of terms that are presumed to be unfair, but that could be justified by the DSP in a particular case on the basis of the circumstances of the case. Where the DSP would not argue that the term is fair, or where the court finds the DSP's argument insufficient, the term is then considered to be unfair indeed. Introducing a black list and/or a grey list would have the additional benefit of shorter court proceedings, as the assessment of the unfairness of a term would be greatly accelerated and the possible finding of a national court that a term is unfair under that court's national contract law would be easier to predict and therefore to anticipate by both parties.

Therefore, **we recommend** the establishment of a black list of forbidden terms and of a grey list of terms presumed to be unfair if these terms are used in a contract with a DSP. Throughout this Study, we have indicated a series of terms that, in our view, should be placed on either the blacklist or the grey list. We will repeat these below in paragraph 5.2. Whether or not these lists should also be applied to other service providers than DSPs or other online traders, is of course a matter for political debate but is not discussed in this Study.

4.2. Damages

A possible consequence of the use of an unfair term is that the trader would be required to pay compensation for damages to the consumer. In a situation where the incorporation of an unfair term into the contract would constitute an unfair commercial practice, the consumer would indeed be entitled to damages under Article 11a UCPD, which provision has been inserted into the UCPD by Article 3(5) MD. In addition, damage could result from the fact that a consumer is required to take legal action or to defend themselves against a claim of the DSP based on the unfair term. Such damage is to be compensated in accordance with national rules on civil procedure. In so far as these rules would render the operation of the UCTD insufficiently effective, these rules would be contrary to the UCTD

[126] Judgment of 14 March 2013, *Aziz*, case C-415/11, EU:C:2013:164, paragraph 69; judgment of 16 January 2014, *Constructora Principado*, case C-226/12, EU:C:2014:10, paragraph 21.

and would therefore be set aside or – if setting aside these rules would not be possible under national law – would constitute a serious infringement of European law and therefore lead to Member State liability. For these reasons, we see no specific need for a legislative action here.

4.3. Termination of contract

The duty for a court not to give any binding effect to an unfair term does not require the national court to annul or terminate the whole of the contract if such an action would be more advantageous to the consumer than merely leaving the unfair term out of consideration. The CJEU clarified, however, that since the UCTD only provides for minimum harmonisation,[127] the Member States are free to determine that the whole contract is to be considered as void if this is more advantageous to the consumer.[128] Such a sanction would have the advantage that DSPs would have a clear incentive to respect the boundaries set by the UCTD.

However, as indicated above, national contract laws differ greatly in these areas where the law has not been fully and exhaustively harmonised. Since the yardstick to determine whether a term is unfair is the extent to which it derogates from the otherwise applicable default rule, the outcome of the unfairness test may differ from one country to the next. Moreover, even under the DSP's own national contract law the outcome of the assessment of unfairness of a term may be uncertain as all circumstances of the case must be taken into account by the court. These different elements are particularly problematic for DSPs that offer their digital services in other Member States than the country in which they have their seat.

For these reasons, we find that an automatic termination of the contract if this is more advantageous to the consumer would be excessive. However, we feel that such a sanction may very well be justified, also in a cross-border situation, in a case where the DSP should have realised the unfairness of the term. This is true, in particular, if the term would feature on the black list of terms that are deemed to be unfair in contracts between DSPs and consumers. The reason for this is that in such a case the DSP could objectively have established that any court would consider the term to be unfair. If the DSP then nevertheless incorporates such a clause in their terms and conditions, it acts in bad faith. A consumer should not be required to continue a relationship with a DSP that has acted in such manner and has thus proven not to be worthy of the consumer's interest in their business. **We recommend** that where a blacklisted term is used in a contract between a DSP and a consumer, and termination of the contract would be more advantageous to the consumer than merely leaving the term out of consideration, the contract would indeed be terminated.

[127] See Article 8 UCTD.

[128] Judgment of 15 March 2012, *Pereničová*, case C-453/10, EU:C:2012:144, paragraph 36.

5. ANALYSIS

5.1. Effectiveness of the current protection framework

As we have previously mentioned in this Study, the current European framework against unfair contract terms may not be an effective consumer protection tool when consumers conclude contracts with DSPs. The main reason for this is the combination of two factors: 1) digital services are often provided cross-border, and 2) the UCTD is a minimum harmonisation measure. These two factors combined may contribute to a different assessment of unfairness occurring in different Member States, creating an uneven level playing field for DSPs and making the enforcement of consumer protection more complex.

Moreover, as this Study has outlined, there are various prevalent commercial practices specific to the online environment, which the drafters of the UCTD could not have taken into account when it was being adopted. As a result, certain clarifications are necessary to improve the consumer protection online against unfair contract terms of DSPs and to provide more legal certainty to DSPs as to what terms and conditions are considered fair.

Consequently, in the following three paragraphs we outline the recommendations that we have made throughout the paper, dividing them into three categories. First, we propose the terms that could be placed on a black list and a grey list of unfair contract terms for DSPs (paragraph 5.2). Second, we recommend certain additional provisions that could be added either to the preamble of the UCTD or its various provisions. Third, we also suggest a few additions to the forthcoming Digital Services Act or a revision of the CRD. These last suggestions follow from issues that we have identified as potentially dangerous to consumer protection in contracts with DSPs, but which are less suited to be regulated in the UCTD itself.

5.2. List of unfair terms in the digital world

In order to increase the effectiveness of the UCTD framework most of our recommendations involve placing various terms on a newly created black list of unfair terms. These would then be terms that would always be prohibited from being added to consumer contracts concluded with DSPs. However, we have also noted a few terms that should instead be presumed to be unfair, unless DSPs prove that under specific conditions of a given contract that term was fair. Therefore, we also provide a short list of possible grey-listed unfair terms.

BLACK LIST OF UNFAIR TERMS IN CONTRACTS WITH DSPS	
Terms which have the object or effect of:	Context
Misleading consumers as to the nature of the contract and statutory rights following from it.	For example, terms that would lead consumers to believe that they are acquiring digital content rather than a digital service, which would limit the applicability of the right of withdrawal (paragraph 1.2.1).
Recognising tacit consent as a valid method of contract's formation.	Such a prohibition would not allow for browse-wrap contracts to be concluded. The unfairness should be recognised regardless whether there was a monetary payment involved (paragraph 2.1.1).
Creating the impression that a DSP acts in a non-professional capacity.	As a result of such a term, consumers would not know that they have a right to rely on the consumer protection framework.

	This prohibition could also be inferred from the current Article 1(b) of the Annex to the UCTD. However, we believe that this prohibition should be made more explicit for contracts concluded with DSPs (paragraph 2.1.2).
Creating the impression that the consumer protection framework does not apply.	This prohibition could also be inferred from the current Articles 1(b) and 1(q) of the Annex to the UCTD. However, we believe that this prohibition should be made more explicit for contracts concluded with DSPs (paragraph 2.1.3).
Allowing DSPs to retain the collected personal data when consumers do not conclude a contract or the DSP terminates the contract.	This prohibition could also be inferred from the current Articles 1(d) and 1(f) of the Annex to the UCTD (paragraph 2.1.4).
Allowing DSPs to collect more personal data throughout the performance of the contract than what parties have originally agreed to, without the DSP notifying consumers about the change of the contract and giving them an option to terminate the contract.	This provision would extend the applicability of Article 1(l) of the Annex to the UCTD to payments with personal data (paragraph 2.1.4). This prohibition could be extended to demand from DSPs to allow consumers to refuse the additional collection of the data and maintain the provision of the old version of the digital services, if the new collection of the data is unnecessary to continue the provision of that service.
Creating the impression that digital services are provided for free, where consumers are paying for the service with their personal data, time or attention.	This provision would legitimise the non-monetary character of payment for the provision of digital services (paragraphs 2.1.4, 2.6).
Creating the impression that digital services are provided "as is".	Such terms mislead consumers as to their statutory rights, where the disturbance in the provision of the service occurred due to the DSP's fault or gross negligence, or the DSP modifying the digital service without a proper notification being provided to consumers or giving them an option to terminate the contract (paragraph 2.2.1).
Preventing consumers from withholding their performance.	This should be prohibited regardless whether the consumers' performance was a monetary or non-monetary payment (paragraph 2.2.1).
Exempting the DSP from liability for consumers' damage caused by any illegal content posted on the DSP's website, if the DSP was informed of that content and did not remove it within a reasonable time, after which time the damage has occurred.	DSPs have an obligation pursuant Articles 12(3), 13(2) or 14(3) ECD to remove any illegal content that they have knowledge of, therefore, they should bear liability for any damage resulting from their inaction (paragraph 2.2.2).
Exempting the DSP from liability for consumers' damage caused intentionally or through gross negligence.	This would not allow DSPs to exclude their liability for example when they did not provide updates to digital services within a reasonable time after they should have discovered the lack of conformity (paragraph 2.2.5).
Allowing DSPs to modify terms, including price, where the contract does not provide a valid reason for the change of terms or the DSP did not inform consumers of the change with reasonable notice before the change was applied, or the consumer has not been informed about the option to and was not given a reasonable time to terminate the contract after having been informed of the change.	This provision would codify the current CJEU case law regarding validity of terms allowing for price modification and extend the application of this rule to other than price contract terms (paragraph 2.2.3).
Hindering the consumers' use of the right of withdrawal.	Such terms could for example: identify the contract as

	pertaining to the provision of digital content rather than digital services; request a reason for the withdrawal; do not clearly identify the model withdrawal form or the method to contact the DSP; place fees on the use of the right of withdrawal (paragraph 2.3).
Providing DSPs with a unilateral right to suspend the performance or terminate a contract, when the consumer's behaviour does not objectively justify this.	This prohibition could also be inferred from the current Articles 1(f) and 1(g) of the Annex to the UCTD (paragraph 2.4.1).
Preventing DSPs from making the data available to consumers after the termination of the contract, within reasonable time after the consumer has requested the termination.	This prohibition would provide an additional incentive for DSPs to comply with their obligations under the GDPR regarding the consumers' rights to be forgotten, to withdraw their consent and the principle of data portability (paragraph 2.4.2).
Prohibiting or penalising negative reviews.	Whilst the practice of prohibiting negative reviews could be considered an unfair commercial practice, terms providing fines for such negative reviews should be declared non-binding on consumers (paragraph 2.8.2).
Misleading consumers as to their non-personalised character.	DSPs should disclose to consumers the use of automated decision-making and which terms have been personalised based thereon (paragraph 2.7.1).
Preventing consumers from being able to contact a human contact point with their complaints and questions.	Aside from the use of virtual assistants and chatbots, consumers should have an option to contact a human (paragraph 2.7.1).
Infringing consumers' rights and data protection principles from the GDPR.	This prohibition could for example prevent DSPs from drafting terms: excluding their liability for the accuracy of the personal data; limiting data storage in an unclear, inaccurate or misleading way; allowing open-ended storage of the personal data; limiting liability for any breach of data security; misleading or deterring consumers from using their right to data portability; limiting the right to withdraw consent for the data collection and processing (paragraph 2.9).
Requiring consumers to go to arbitration or suggesting that arbitration is the only method available for dispute resolution.	Such terms either dispose of or create an impression with consumers that their right to pursue the judicial enforcement of their rights is limited or even excluded (paragraph 2.10.1).
Derogating from Brussels I Regulation (recast) on forum choice.	Such terms may discourage consumers from pursuing their rights through judicial enforcement by making them believe they cannot claim their rights in the court that has jurisdiction for their place of residence (paragraph 2.10.2).
Misinforming consumers as to their right to rely on the mandatory consumer protection of the country where they live.	Such terms may discourage consumers from pursuing their rights through judicial enforcement, as they may not be aware of the rights that they enjoy (paragraph 2.10.3).

GREY LIST OF UNFAIR TERMS IN CONTRACTS WITH DSPS	
Terms which have the object or effect of:	Context
Discriminating against consumers as a result of the	Personalisation of terms may but does not have to lead

personalisation of such terms.	to discrimination of consumers. However, we believe that it is a DSP that should have a burden of proof that a personalised term is not discriminating against the consumer (paragraph 2.7.2).
Informing consumers of their rights and obligations through the use of hyperlinks.	Layering of the information may have beneficial effects, e.g. it may limit the negative effects of the information overload. However, placing terms and conditions behind a hyperlink may dispose consumers of the 'real opportunity' to read them. Therefore, DSPs should have the burden of proof that they drew the consumers' attention to terms and conditions that have been 'hidden' behind a hyperlink (paragraph 2.1.1).
Limiting or excluding the access to digital services, if consumers do not give an explicit consent to the sharing of personal data in the scope exceeding what is needed for the provision of a digital service, including as a counter-performance for the provision of digital services.	This presumption of unfairness would give effect to the data minimisation principle in the GDPR (paragraph 2.7.3). It needs to be emphasised here that we consider as 'necessary' such a provision of personal data that allows DSPs not only to functionally provide the digital service, but also corresponds to the DSP's business model. DSPs will need to justify why the limitation of access to digital services was justified in a case by showing that the collection of consumers' data was necessary either as counter-performance or to functionally provide the services.
Providing DSPs with a license to use the user-generated content unless this has been brought specifically to the consumers' attention at the moment of the contract's conclusion and has been individually, separately and explicitly accepted by consumers.	In most cases, DSPs draft terms giving them very broad licenses to use the user-generated content, with consumers often not realising that they will not be able to retrieve this content in the future. Such terms should thus be presumed unfair unless the DSP justifies why under the given circumstances the granting of the license was justified (paragraph 2.11.1).
Forming a no-survivor clause.	DSPs need to provide a valid justification for excluding the rights of consumers to digital inheritance (paragraph 2.5).

5.3. Recommendations for the UCTD framework

Our Study shows that the adoption of a blacklist and a greylist of unfair contract terms should raise the effectiveness of consumer protection in contracts concluded with the DSPs. However, we also recommend the following changes in the UCTD:

Suggested amendment to the UCTD	Context
In the preamble: explicitly acknowledging that non-monetary payment, including but not limited to the provision of personal data, is one of the obligations of consumers in contracts concluded with DSPs. This obligation should weigh in on the assessment of the balance between the parties' rights and obligations in the unfairness test.	As the unfairness test considers a particular term in light of all rights and obligations of the parties, and a balance between them, it is important to acknowledge consumers' non-monetary contributions, as well, especially where they drive the business model of DSPs (paragraph 2.6.1).
In the preamble: explicitly acknowledging that personalised terms remain within the scope of the unfairness test, unless the limitations applying to core terms are of relevance here.	This would help avoiding any uncertainty regarding the applicability of the UCTD to personalised terms and confirm the presumption of their character as still non-individually negotiated terms (paragraph 2.7.4).

In the preamble: explicitly acknowledging that where terms and conditions pertain to the supply of the personal data, both provisions of the UCTD and of the GDPR apply and are complementary.	This would clarify the obligations for DSPs collecting and processing the personal data of consumers, as well as facilitate the enforcement of both protection frameworks for the appropriate authorities (paragraph 2.11.2).
In the preamble: explicitly acknowledging that the assessment of the compliance with the principle of transparency may require different considerations for online and offline terms.	This would clarify for the enforcement authorities the need to consider different options for the design of consumer information online, e.g. regarding layering of the information, attracting the consumers' attention to it (paragraph 3.1).
In the preamble or in Article 5 UCTD: explicitly acknowledging that the assessment of the compliance with the principle of transparency requires checking the language of the disclosure.	Especially where DSPs target consumers in a country other than where the DSP has their seat of business, we would consider terms to be transparent only where they are provided in at least one official language of the country of residence of the consumer (paragraph 3.3).
Article 3(3) and Annex to the UCTD: change the indicative list of potentially unfair terms into a black list of terms that under all circumstances are considered unfair, at least in a consumer contract with a DSP.	The current indicative list of potentially unfair terms falls short, in particular in case of consumer contracts, in sufficiently protecting the interests of consumers and providing legal certainty for DSPs. Changing the indicative list into a black list will provide better consumer protection, offer more legal certainty to DSPs, and help create a level playing field between DSPs.
Article 6 UCTD: introduce a rule that if a DSP drafted a term, which is on the black list of unfair terms, and its removal from the contract would be less advantageous to consumers than declaring a contract void, the whole contract should be terminated.	We propose introducing this rule, as its harsh sanction could be an effective deterrent for DSPs to draft such unfair terms. Whereas in the case of the open clause of Article 3(1) UCTD and of terms on the grey list, the DSP may have believed in good faith that the term found to be unfair was (in their specific case) not unfair, such belief is clearly unjustified, and the DSP has acted in bad faith, if it concerns a term on the black list. As the black list of unfair terms would be well-known to DSPs, they will easily be able to protect themselves from this sanction.

In addition, we recommend further research being conducted and resources being allocated to support the development of 'two-sided' terms, *ex ante* testing of terms and conditions, and trustmarks (paragraph 3.2).

5.4. Other recommendations

As our Study has showed the following obligations for the DSPs should be regulated further:

Obligation of a DSP	Context
To transparently inform consumers what constitutes terms and conditions.	Terms and conditions are often provided online on various web pages and are frequently entitled in a way that does not suggest these pages contain such terms (paragraph 1.2.2).
To ask for the consumers' explicit consent to the contract's conclusion and to the terms and conditions, prior to a contract's conclusion.	There should not be a possibility for online contracts to be concluded through tacit consent. This obligation will also oblige platforms to reveal to consumers if they have a contract with them, even if only for the provision of an intermediary service (paragraph 2.1.1).
To draw the consumers' attention to terms and conditions.	It is easy to overlook DSPs terms and conditions amongst various web pages that are available on their main

	websites (paragraph 2.1.1).
To transparently inform consumers whether the mandatory consumer protection framework is applicable.	This is a positive obligation for DSPs to confirm to consumers that they are concluding a B2C transaction, which offers them a specific protection framework (paragraph 2.1.3).
To transparently inform consumers that the automated decision-making mechanisms are in use and to facilitate human contact points for consumers, as well as human oversight over automated decision-making mechanisms.	This obligation should pertain to any use of automated decision-making that has an impact on terms and conditions of the contract, not only in relation to its influencing the price for digital services. This would help prevent discrimination of consumers on the basis of personalised contract terms, making them aware of such a personalisation and encouraging seeking explanations for it as well as alternative offers (paragraph 2.7.1).
To use icons and graphical aids to convey information, whenever reasonable.	This should help increase transparency of terms and conditions, as well as of other consumer information (paragraph 3.1.1).

These obligations could be added to the forthcoming Digital Services Act or a further revision of the CRD could be considered. It went beyond the scope of this Study to consider whether these obligations should only pertain to the DSPs or also to other online traders. We recommend that before any such obligations are introduced a further study is conducted to give an answer to this question.

Moreover, we would suggest the addition of a specific obligation for online marketplaces to verify the data provided by the DSPs, as far as reasonable, on whether the DSPs are acting in a non-professional capacity on the marketplace. This would further extend the obligations of the online marketplaces as currently provided in Article 6a (1) CRD, as introduced by the MD (paragraph 2.1.2).

Finally, we would suggest the introduction in the EU law framework of default rules regarding limitation of data storage for DSPs. This would oblige DSPs to remove the collected consumer data within reasonable time from the moment such data becomes unnecessary for the provision of their services. Such default rules would be necessary if the terms for data storage limitations of DSPs are considered unfair and, therefore, are non-binding. Not regulating this on the EU level, will likely lead to the adoption of different time limits by the Member States, further contributing to the legal uncertainty on the market for the provision of digital services.

6. CONCLUSIONS

As the UCTD is a minimum harmonization directive and DSPs often provide their services cross-border, the current European framework against unfair contract terms may not be an effective consumer protection tool when consumers conclude contracts with DSPs. As a result, DSPs may be confronted with a different assessment of unfairness in different Member States, creating an uneven level playing field for DSPs. Moreover, enforcement agencies and consumer organizations face complications in the enforcement of consumer protection as a result of these factors. Given the fact that the UCTD framework was developed for the offline world and consumer contracts concluded online with DSPs were non-existing at that time, it is necessary to amend the UCTD to, on the one hand, improve consumer protection online against unfair contract terms of DSPs and, on the other hand, to provide more legal certainty to DSPs as to what terms and conditions are considered fair.

In this Study, we have recommended that the current indicative list of potentially unfair terms be turned into a black list of terms that under all circumstances should be considered unfair if these terms are included in a contract between a consumer and a DSP. This will provide better consumer protection, offer more legal certainty to DSPs, and help create a level playing field between DSPs. In addition, we have identified several terms that currently are being used by DSPs that, in our view, are always or almost always unfair when used in contracts concluded with consumers, but that are not reflected or can only indirectly be linked to items on the current indicative list. We recommend that these terms should be placed on a black list of forbidden terms or on a grey list of terms presumed to be unfair if these terms are used in a contract with a DSP. Whether or not these lists should also be applied to other service providers than DSPs or other online traders, is of course a matter for political debate but is not discussed in this Study. We have also recommended strengthening the sanction for the DSP's use of terms that, without any doubt, are unfair. In this respect, we have recommended to add a paragraph to Article 6 UCTD to provide that where a DSP has used a term, which is on the black list of terms that under all circumstances is forbidden, courts should be allowed to terminate the whole contract if this sanction is more advantageous for the consumer than merely removing the unfair term from the contract.

Further, we recommend introducing new obligations for DSPs pertaining to the conclusion of contracts and the incorporation of terms and conditions, and to promoting transparency of terms and conditions, of information regarding consumer protection rules, and of the application of automated decision-making mechanisms. These obligations could be added to the Digital Services Act or a further revision of the CRD could be considered. Finally, in order to prevent the adoption of different time limits by the Member States and therefore further legal uncertainty on the market for the provision of digital services, we suggest the introduction of EU-wide default rules regarding limitation of data storage for DSPs requiring DSPs to remove the collected consumer data within reasonable time from the moment such data becomes unnecessary for the provision of their services.

REFERENCES

- Adshead, A., 'IT Priorities 2020: Covid-19 consolidates storage push to cloud', *Computer Weekly*, 10 November 2020, <https://www.computerweekly.com/news/252491828/IT-Priorities-2020-Covid-19-consolidates-storage-push-to-cloud> accessed 20 November 2020.
- Alkazemi, M.F., Van Stee, S.K., 'Electronic direct-to-consumer advertising of pharmaceuticals: an assessment of textual and visual content of websites', *Health Education Research*, Vol. 35, 2020, 134-151.
- Bakos, Y., Marotta-Wurgler, F., Trossen, D.R., 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts', *The Journal of Legal Studies*, Vol. 43, 2014, pp. 1-35.
- BEUC, 'Euroconsumers launch a collective action against Facebook', *BEUC News*, 31 May 2018, <https://www.beuc.eu/press-media/news-events/euroconsumers-launch-collective-action-against-facebook>.
- BEUC, 'ENISA advisory group points to lack of security in consumer IoT', *BEUC News*, 29 October 2019, <https://www.beuc.eu/press-media/news-events/enisa-advisory-group-points-lack-security-consumer-iot>.
- Bol, N., and others, 'Vulnerability in a Tracked Society: Combining Tracking and Survey Data to Understand Who Gets Targeted with What Content', *New Media & Society,* Vol. 22, 2020, pp. 1996-2017.
- Bourreau, M., de Streel, A., 'The regulation of personalised pricing in the digital era', *OECD publication*, 25 September 2020, DAF/COMP/WD(2018)150

  <https://one.oecd.org/document/DAF/COMP/WD(2018)150/en/pdf>.
- Bradshaw, S., Millard, C., and Walden, I., 'Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services', *International Journal of Law and Information Technology*, Vol. 19, 2011, 187–223.
- Busch, C., and others, 'The ELI Model Rules on Online Platforms', *Journal of European Consumer and Market Law*, Issue 2, 2020, 61-70.
- Djonov, E., 'Website Hierarchy and the Interaction between Content Organization, Webpage and Navigation Design: A Systemic Functional Hypermedia Discourse Analysis Perspective', *Information Design Journal*, Vol. 15, 2007, 144-162.
- Ducato, R., Strowel, A., 'Information Duties between Consumer and Data Protection in the "Internet of Platforms": Promoting Awareness by Design', *Droit de la consommation*, Vol. 122-123, 2019, 123-149.
- Ebers, M., 'Legal Tech and EU Consumer Law', in: Michel Canarsa/Mateja Durovic/Francisco de Elizalde/Larry di Matteo/André Janssen/Pietro Ortolani (eds.), *Lawyering in the Digital Age*, Cambridge: Cambridge University Press, 2021, as published online (preprint), available at https://ssrn.com/abstract=3694346 18 (last visited 18 November 2020).
- Elshout, M., and others, 'Study on consumers' attitudes towards Terms and Conditions (T&Cs). Final report' , 2016,

  https://ec.europa.eu/info/sites/info/files/terms_and_conditions_final_report_en.pdf> accessed 20 November 2020.

- European Commission, 'Consumer market study on online market segmentation through personalised pricing/offers in the European Union. Executive Summary', June 2018, <https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/exec_summary_online_personalisation_study_en.pdf>.
- Forbrukerrådet, 'Appfail. Threats to Consumers in Mobile Apps', March 2016a, <https://fil.forbrukerradet.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf>.
- Forbrukerrådet, 'Fitness wristbands violate European law', 3 November 2016b, <https://www.forbrukerradet.no/side/fitness-wristbands-violate-european-law/>.
- Forbrukerrådet, 'Connected toys violate European consumer law', December 2016c, <https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/>.
- Forbrukerrådet, 'Critical security flaws remain in smartwatches for kids', 7 December 2017, <https://www.forbrukerradet.no/side/critical-security-flaws-remain-in-smartwatches-for-kids/>.
- Garcia, M., 'Browsewrap: A Unique Solution to the Slippery Slope of the Clickwrap Conundrum', *Campbell Law Review*, Vol. 36, 2014, 31-74.
- Gardiner, C., *Business to Consumer Contracts in the Electronic Marketplace: Striking a Proper Balance between Private and Public Regulatory Objectives*, PhD thesis at University College Cork, Ireland, March 2019, <https://cora.ucc.ie/handle/10468/7958> accessed 20 November 2020.
- Haucap, J., 'The Facebook Decision: First Thoughts by Haucap', 7 February 2019, <https://www.d-kart.de/blog/2019/02/07/the-facebook-decision-first-thoughts-by-haucap/> accessed 20 November 2020.
- Helberger, N., Zuiderveen Borgesius, F., and Reyna, A., 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law', *Common Market Law Review*, Vol. 54, 2017, 1427-1466.
- Helberger, N., and others, 'EU Consumer Protection 2.0: Surveillance, consent and the vulnerable consumer. Regaining citizen agency in the information economy', *BEUC study*, 2020.
- Hogarth, J.M., Merry, E.A., 'Designing Disclosures to Inform Consumer Financial Decisionmaking: Lessons Learned from Consumer Testing', *Federal Reserve Bulletin*, 2011, <https://ideas.repec.org/a/fip/fedgrb/y2011iaugustnv.97.html> accessed 20 November 2020.
- Jabłonowska, A., and others, 'Consumer law and artificial intelligence. Challenges to the EU consumer law and policy stemming from the business' use of artificial intelligence', *EUI Working Papers LAW*, Vol. 11, 2018, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228051> accessed 20 November 2020.
- Junuzović, M., 'Transparency of (Pre-)Contractual Information in Consumer Credit Agreements: Is Consistency the Missing Key?', *Croatian Yearbook of European Law and Policy*, Vol. 14, 2018, 69-98.
- Kaptein, M., *Persuasion Profiling: How the internet knows what makes you tick*, Business Contact, 2015.
- Kaptein, M., and others, 'Personalizing Persuasive Technologies: Explicit and Implicit Personalization Using Persuasion Profiles', *International Journal of Human-Computer Studies*, Vol. 77, 2015, 38-51.
- Kulesza, M., 'Italian court says Facebook isn't free', *In principle*, 13 February 2020, <http://www.codozasady.pl/en/italian-court-says-facebook-isnt-free/>.

- Leone, C., 'Transparency revisited—on the role of information in the recent case-law of the CJEU', *European Review of Contract Law*, Vol. 10, 2014, 312–325.
- Leone, C., 'French tribunal invalidates many terms in Google+ T&Cs', *Recent developments in European Consumer Law*, 14 February 2019, <http://recent-ecl.blogspot.com/2019/02/french-tribunal-invalidates-many-terms.html>.
- Lester, P., 'Fake reviews make consumers more than twice as likely to choose poor-quality products', *Which? News*, 29 May 2020, <https://www.which.co.uk/news/2020/05/the-real-impact-of-fake-reviews/> accessed 1 December 2020.
- Loos, M, Helberger, N., Guibault, L., and Mak, C., 'The regulation of digital content contracts in the Optional Instrument of contract law', *European Review of Private Law*, Vol. 6, 2011, 729-758
- Loos, M., and Luzak, J., 'Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers', *Journal of Consumer Policy*, Vol. 39, 2016, 63-90.
- Loos, M.B.M., 'Transparency of Standard Terms under the Unfair Contract Terms Directive and the Proposal for a Common European Sales Law', *European Review of Private Law*, Vol. 2, 2015, 179-193.
- Loos, M.B.M., 'The Modernization of European Consumer Law: A Pig in a Poke?', *European Review of Private Law*, Vol. 1, 2019, 113-134.
- Luzak, J., 'To Withdraw Or Not To Withdraw? Evaluation of the Mandatory Right of Withdrawal in Consumer Distance Selling Contracts Taking Into Account Its Behavioural Effects on Consumers', *Journal of Consumer Policy*, Vol. 37, 2014, 91-111.
- Luzak, J., 'Doprecyzowanie Zasady Transparentności w Polskim Prawie Konsumenckim', *Studia Prawa Prywatnego*, Vol. 1, 2020a, 41-62.
- Luzak, J., 'The Steady Creep of an Average Consumer as a Reference Consumer in the Assessment of the Transparent Provision of Mandatory Information', *Tijdschrift voor Consumentenrecht & handelspraktijken (TvC)*, Vol. 5, 2020b, 265-274.
- Luzak, J., 'Tailor-made Consumer Protection: Personalisation's Impact on the Granularity of Consumer Information', in: Corrales, M., Haapio, H., Hagan, M., and Doherty, M., *Legal Design: Integrating Business, Design and Legal Thinking with Technology*, Edward Elgar, 2021 (forthcoming), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3696483>.
- Mattioli, D., 'On Orbitz, Mac Users See Costlier Hotel Options', *Wall Street Journal*, 23 August 2012, <https://www.wsj.com/articles/SB10001424052702304458604577488822667325882>.
- Micklitz, H.-W., 'Reforming European unfair terms legislation in consumer contracts', *European Review of Contract Law*, Vol. 4, 2010, 347–383.
- Mik, E., 'The erosion of autonomy in online consumer transactions', *Law, Innovation and Technology*, Vol. 8, 2016, 1-38.
- Mitchell, V., 'What if the companies that profit from your data had to pay you?', *The Conversation*, 30 July 2018, <https://theconversation.com/what-if-the-companies-that-profit-from-your-data-had-to-pay-you-100380>.
- Pavis, M., 'Things come in threes – Paris Tribunal guts Facebook's T&C's', *IP Kitten Blog*, 6 May 2019, <https://ipkitten.blogspot.com/2019/05/things-come-in-threes-paris-tribunal.html>.

- Podszun, R., 'Die Facebook-Entscheidung: Erste Gedanken von Podszun', 8 February 2019, <https://www.d-kart.de/blog/2019/02/08/die-facebook-entscheidung-erste-gedanken-von-podszun/> accessed 20 November 2020.
- Podszun, R., 'Facebook Case: The Reasoning', 28 August 2020, <https://www.d-kart.de/en/blog/2020/08/28/facebook-case-the-reasoning/>.
- Quarta, A., 'Narratives of the Digital Economy: How Platforms Are Challenging Consumer Law and Hierarchical Organization', *Global Jurist* , Vol. 20, 2020,

  <http://www.degruyter.com/view/journals/gj/20/2/article-20200026.xml>.
- Que Choisir, 'L'UFC-Que Choisir obtient la condemnation de Google, *Que Choisir*, 13 February 2019, <https://www.quechoisir.org/action-ufc-que-choisir-donnees-personnelles-l-ufc-que-choisir-obtient-la-condamnation-de-google-n63567/>.
- Reyna, A., 'The Price Is (Not) Right: The Perils of Personalisation in the Digital Economy', *InformaConnect*, 4 January 2019, <https://informaconnect.com/the-price-is-not-right-the-perils-of-personalisation-in-the-digital-economy/>.
- Rossi, A., and others, 'When Design Met Law: Design Patterns for Information Transparency', *Droit de la consummation*, Vol. 122-123, 2019, 79-121.
- Rustad, M., and Onufrio, M.V., 'Reconceptualizing consumer terms of use for a globalized knowledge economy', *University of Pennsylvania Journal of Business Law*, Vol. 14, 2012, 1085–1190.
- Schulte-Nölke, H., and others, 'Discrimination of Consumers in the Digital Single Market', *Study for the European Parliament's Committee on Internal Market and Consumer Protection (IMCO)*, November 2013, IP/A/IMCO/ST/2013-03,

  <https://www.europarl.europa.eu/meetdocs/2014_2019/documents/imco/dv/discrim_consumers_/discrim_consumers_en.pdf>.
- Seizov, O., Wulf, A.J., 'Communicating Legal Information to Online Customers Transparently: A Multidisciplinary Multistakeholderist Perspective', *Journal of International Consumer Marketing*, 2020, 1-19.
- Seizov, O., Wulf, A.J., Luzak, J., 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU', *Journal of Consumer Policy*, Vol. 42, 2019, 149-173.
- Sheng, X., and others, 'Sight Unseen: The Role of Online Security Indicators in Visual Attention to Online Privacy Information', *Journal of Business Research*, Vol. 111, 2020, 218-240.
- Shi, S.W., Xia, M., and Huang, Y., 'From Minnows to Whales: An Empirical Study of Purchase Behavior in Freemium Social Games', *International Journal of Electronic Commerce*, Vol. 20, Issue 2, 2015, 177-207.
- Shiller, B., 'First-Degree Price Discrimination Using Big Data', *EconPapers*, Working Paper from Brandeis University No 58, 2014,

  <https://www.brandeis.edu/economics/RePEc/brd/doc/Brandeis_WP58R2.pdf>.
- Simmonds, E., 'Amazon 'betraying trust' of millions of consumers with flawed Amazon's Choice endorsement', *Which? News*, 6 February 2020, <https://www.which.co.uk/news/2020/02/amazon-flawed-amazons-choice-endorsement/> accessed 1 December 2020.

- Study Group on a European Civil Code and the Research Group on EC Private Law (Acquis Group), *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR). Outline Edition*, Sellier, 2009.
- Susser, D., Roessler, B., Nissenbaum, H.F., 'Online Manipulation: Hidden Influences in a Digital World', *Georgetown Law Technology Review*, Vol. 4, 2019, 1-45.
- Tenreiro, M, 'The community directive on unfair terms and national legal systems. The principle of good faith and remedies for unfair terms', *European Review of Private Law*, Vol. 3, 1995, 273–284.

This study analyses common terms in contracts of digital service providers, indicating when they could significantly distort the balance between the parties' rights and obligations to the detriment of consumers and should, therefore, fall within the scope of the Unfair Contract Terms Directive. Further, the study discusses the particularities of the assessment of online transparency of terms of digital service providers and sanctions they could face if they breach the current consumer protection framework. Recommendations are made to improve the effectiveness of this framework by: introducing a black and grey list of unfair terms, strengthening current sanctions, and introducing new obligations for digital service providers.

PE 676.006
Print ISBN 978-92-846-7696-5| doi: 10.2861/824264| QA-04-21-020-EN-C
PDF ISBN 978-92-846-7697-2| doi: 10.2861/7890| QA-04-21-020-EN-N