Kaspar Kala

Analysis on the Remedial Situation of Cloud Contracts from a Consumers’ Perspective

Master thesis

Supervisor

Prof. Dr. Kees Stuurman

Tilburg

2014
Table of Contents

1. Analysis on the Remedial Situation of Cloud Contracts from a Consumers’ Perspective…………………………………………………………………………………………………….4
  1.1 Background ..................................................................................................................................................................................................................4
  1.2 Research question, Methodology and the Organisation of the Thesis .........................................................6
  1.3 Significance ..................................................................................................................................................................................................................11

2. Characteristics of a Cloud Contract ..................................................................................................................................................................................................12
  2.1 Cloud Computing ........................................................................................................................................................................................................12
  2.2 Imbalance of Negotiation Powers ....................................................................................................................................................................................15
    2.2.1 Standard term contracts – a feasible and balanced method of contracting at present day? ... ........................................................................................................................................................................................................15
    2.2.2 Who are influenced by the state of disequilibrium? .........................................................................................................................16
  2.3 “Click-Through/Click-Wrap Contracts” .................................................................................................................................18
  2.4 “Vendor Lock-in” .........................................................................................................................................................................................................21
  2.5 Characteristics of a Cloud Contract - Findings .................................................................................................................................22

3. Analysing the Cloud Contract’s Terms and Conditions in the Light of Consumer Law. 23
  3.1 Definitions of a “Consumer” and an “Average Consumer” ..........................................................................................24
    3.1.1 Rationale on consumer protection ..................................................................................................................................................................................25
    3.1.2 Rationale to (or not to) protect businesses against unfair terms .......................................................................................................................27
  3.2 Relevant Directives for Cloud Contracting ................................................................................................................................................................................28
    3.2.1 The Unfair Terms Directive – 93/13/EEC (UTD) ..........................................................................................................................................................................................28
    3.2.2 Directive 2005/29/EC concerning unfair B2C commercial practices (UCP) …33
    3.2.3 Directive 2011/83/EC, Consumer Rights Directive (CRD) ............................................................................................................................33
    3.2.4 Directive 2000/31/EC – on electronic commerce (ECD) ..........................................................34
  3.3 Analysis on the Terms and Conditions ..................................................................................................................................................................................................36
    3.3.1 Infrastructure as a Service platform providers – Dropbox and UKFast ..........37
    3.3.2 Platform as a Service providers – Google Apps for Business and Windows Azure.................................................................................................................................44
3.3.3 Software as a Service platform providers – Salesforce.com and Dell Boomi...48

3.4 Consumer Protection Regime in Estonian Law ..................................................50

3.4.1 Unfair terms of six service providers through the prism of Estonian consumer law................................................................................................................52

3.5 Consumer Protection and UK law.................................................................55

3.5.1 Unfair Contract Terms Act (UCTA), 1977......................................................55

3.5.2 Sale of Goods and Services Act (SGSA), 1982..............................................56

3.5.3 The Unfair Terms in Consumer Contracts Regulations (UTCCR), 1999........57

3.5.4 Unfair standard terms under the UCTA, SGSA and UTCCR ......................57

3.6 Findings and Opinion......................................................................................59

4. Soft law and Assurances .................................................................................64

4.1 Cloud Industry Forum (CIF) ........................................................................67

4.1.1 Introduction.................................................................................................67

4.1.2 Moving the Cloud Industry Forum Code of Practice’s principles to practice – Is Cloud Industry Forum the true champion of trust and transparency? .................70

4.2 Cloud Security Alliance’s (CSA) Security, Trust & Assurance Registry (STAR) initiative ............................................................................................................73

4.3 The Adverse case of TRUSTe.........................................................................75

4.4 Assurance seals – Sufficient Ameliorate for the Remedial Situation?.........77

5. Conclusion ........................................................................................................79

Bibliography ........................................................................................................83
1. **Analysis on the Remedial Situation of Cloud Contracts from a Consumers’ Perspective**

1.1 **Background**

Cloud computing is an eminently actual topic. Billions of people are using it – knowingly or inadvertently. Homepage of the European Commission positions that cloud computing is “the next big evolution for the Internet” and this is a space “where everyone from individuals to major corporations and governments move their data storage and processing into remote data centres.”¹ There is no reason to object this statement because ever more people are and will be in the “cloud” in the years to come. Cloud computing is all about processing of data² and this thesis will take into account the inference of the information society, which results in the increasing awareness of data protection issues by the consumers and the knowledge that their data is being used by cloud providers for business purposes. But, this thesis does not concentrate on the data protection issues, rather focuses on the remedial situation between the users and providers of the cloud service. Still, the increase in awareness concerning the fact that our data is shared with companies is an important factor and cannot be left unnoticed.

Also, the thesis will not focus on the potential future benefits of cloud computing but instead concentrates on the present situation. The scope of this master thesis is to analyse the remedies in cloud contracts from a consumer perspective. Besides consumers, the thesis also turns to SMEs³ who, as argued below, suffer from the same facets of concluding cloud contracts online.

Remedies in the cloud contracts are a representation of the interplay between standard form contracts, inequality of bargaining power and consumer protection.

---


² Processing is “...any operation or set of operations which is performed upon personal data...”, art 2(b) of Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 p. 31 – 50.

³ According to article 2(1) of the Annex of the Commission Recommendation of May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC), OJ L 124/34, 20.05.2003, SMEs (comprising of micro, small and medium-sized enterprises) are companies which employ fewer than 250 persons and which have an annual turnover not exceeding 50 million euros. According to article 2(2), a small enterprise employs fewer than 50 persons and the annual turnover does not exceed 10 million euros. Microenterprise (article 2(3)) employs fewer than 10 persons and the annual turnover does not exceed 2 million euros.
The idea is that the principle of freedom of contract allows drawing up of unequal terms in the standard term contracts where cloud service providers (hereinafter providers) can exploit their superior negotiation power. Therefore, contract law is not the most suitable tool for consumer protection\textsuperscript{4} – consumer protection legislation is needed. Nevertheless, the author emphasizes the necessity to reduce the imbalance situation in the standard terms and conditions (T&Cs) to improve the remedial situation for consumers and SMEs. Remedies should be seen from a substantive aspect and they should counteract or make good any harmful events. A remedy must be a cogent one, meaning that it must provide the consumer with enforceable tools for redress. Thus, a remedy must be “effective.” An “effective” remedy requires that access to it is free – no arbitrary barriers exist to seek redress. These impediments may take the form of costs, time and insufficient access to information. Lack of transparency is a material failure and is a definite barrier to redress. Consequently, the remedial situation is analysed through the terms of governing law and jurisdiction, modification and variation, assignment and termination. Also, the thesis will focus on a clear-cut cases of abuse of bargaining power on behalf of the providers.

1.2 Research question, Methodology and the Organisation of the Thesis

This paper undertakes to answer the question if the remedial situation between the provider and the consumer/SME is an “effective” one? The thesis will divide the remedial clauses to four segments: terms relating to transparency; time; cost and abuse. These segments will be henceforth referred to as “criteria of effectiveness.” The criteria represent barriers to an effective remedy. Transparency is seen as the most important and at the same time, the most difficult aspect of “effectiveness.” Transparency refers to the provision of insufficient information which is used by the provider to gain an advance in a hypothetical dispute. This is important because enforcement of remedial clauses by the consumer/SME is dependent on the party knowing his rights, being able to afford to enforce them, considering the cost and time involved to do this.\(^5\) If the contract does not provide clarity about, e.g. the termination process, the customer of a cloud service provider is unable to assess the abovementioned factors. Timeframe to initiate proceedings is a factor for enforcing the rights under a cloud contract. Also, knowing that the remedial process is too lengthy or complicated, (both, money and/or time-wise) it implicates that the consumer and/or a SME is unable to enforce his rights under the contract.

To provide an illustration of the remedial situation, the thesis focuses on the terms and conditions (T&C) of six cloud providers which will be analysed in detail through the lens of the four remedial segments described above and through the relevant consumer protection law. The six providers analysed are: Dropbox and UKFast; Google Apps for Business and Windows Azure; Salesforce.com and Dell Boomi. The thesis will exclude from its scope “free” cloud contracts and will only deal with paid services, because notions “free” and “paid” would require further analysis than one would anticipate at first sight and it is an unsettled question if the cloud provider has the same duty of care\(^6\) when the user can use the service without paying for the subscription.\(^7\)

\(^7\) Also, this thesis will not focus on the issue of how “free “a free cloud contract really is. Addressing these issues – A. Cunningham and C. Reed, “Caveat Consumer? – Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud” (January 18, 2013), Queen Mary School of Law Legal Studies Research Paper No.
Dropbox and UKFast are examples of infrastructure as a service (IaaS) platform. This platform is the most common to a consumer who wishes to store data in the cloud. The two providers were taken as subject to analysis because Dropbox has more than 200 million users world-wide and UKFast is certified by the Cloud Industry Forum while Dropbox is not. Cloud Industry Forum’s Code of Practice (CIF’s CoP) is a soft law instrument to enhance transparency in the T&Cs of the cloud service providers (see 4.1 below). This offers a possibility to compare the transparency and accessibility issues of these two providers. Google Apps for Business and Windows Azure are examples of platform as a service (PaaS) providers. Google Apps for Business is subject to analysis because it is mainly targeted towards small and medium sized enterprises (SMEs) with IT departments and Google is one of the biggest cloud service providers. Windows Azure is the main competitor of Google in this field. Salesforce.com and Dell are the examples of software-as-a-service (SaaS) cloud offering model. Salesforce.com is known for its CRM service. Dell Boomi, on the other hand, is not that well-known. Dell Boomi provides an on-demand multi-tenant cloud integration platform for connecting cloud and on-premises applications and data. The platform enables customers to design cloud-based integration processes called Atoms and transfer data between cloud and on-premises applications. Dell is also a member of the CIF’s CoP. Thus, the six cloud providers are divided equally (2:2:2) based on the cloud offering model (IaaS, PaaS and SaaS). Five service providers – Google, Dropbox, Microsoft, Dell and Salesforce.com – out of six are based in the United States while only UKFast resides in the EU (in the United Kingdom).


9 Cloud Industry Forum (CIF) provides a Code of Practice the providers have to adhere to and cater transparency and better consumer protection. See <http://www.cloudindustryforum.org/end-users/code-of-practice-and-the-consumer/> accessed 29 November 2013. CIF promotes itself as being the facilitator of transparency in the cloud environment. Thus, it is necessary to analyse the efficacy of such a self-regulatory instrument.


11 Salesforce.com has more than 2,100,100 subscribers. See <http://salesforceprogrammers.com/article467-History_of_Salesforce_.html>


The second chapter of the paper will analyse the characteristics of cloud contracts between a consumer/SME and a cloud service provider. Keyword here is negotiating power – specifically, abuse of it by the providers – which leads to imbalanced contracts with uneven risks when entering into a contract. It is clear that consumers cannot negotiate terms with the cloud provider. However, SMEs are usually in the similar “take it or leave it” situation; consequently they are also included in the analysis.

The second chapter will also focus on the aspect of cloud contracts being “click-through” contracts. This concept means that the customer has to accept the provider-friendly terms and conditions prior to using the service. This invokes the problem of informed consent provided by the consumer/SME while concluding the contract because without clicking “yes, I agree” the customer cannot use the service. The mean length of the T&Cs lure consumers/SMEs to give consent to these T&Cs and to accept the offered remedial situation.

Subsequently, the second chapter will discuss the “vendor lock-in” issue. The term “lock-in” is used to refer to a situation where a customer (being a consumer or SME) has significant difficulties (time or money-wise) to change from one provider to another. Locking-in the customer is the goal of every service provider. This is something that is not written in any of the T&Cs, but is achieved by technical steps. Imbalanced remedial clauses in the T&Cs may aggravate the lock-in problem, e.g. in case of terms which do not provide refunds and help to migrate data in case of contract termination.

The third chapter of the thesis focuses on the remedies the providers are offering to the customers in its T&Cs. The question here is if the remedies in cloud contracts meet the criteria of “effectiveness”? This part analyses relevant consumer protection laws of the European Union\textsuperscript{14} and examines the offered remedies in standard form cloud contracts through the prism of consumer protection. The imbalanced terms

give an impression of inequality and consumer protection provides a shield against these unfair contract terms – unfair terms are not binding to consumers.\textsuperscript{15} If a standard term confers jurisdiction away from the residence of the consumer, consumer law reassigns jurisdiction in the domicile of the consumer.

The third chapter also takes a comparative approach and gives an overview of the consumer protection regime of Estonian and United Kingdom’s law. These two countries provide an interesting comparison because Estonian law has embraced the approach where contract terms in a business-to-business (B2B) contract may also be considered unfair while UK law has developed a restrictive notion of “business dealing as a consumer” which cover very limited number of cases and does not offer similar protection when a SME is contracting to a multinational company.

Analysing the criteria of effectiveness of the remedial clauses provides a view of how the risks of entering into a contract are divided. This risk allocation proposal is an important part of the thesis because the main objective of this paper is not only to contribute to consumer awareness, but to raise cloud providers’ attention to the fact that they can also benefit from transparency and balanced T&Cs.\textsuperscript{16} If the remedial process is poorly designed (which is the hypothesis for the current situation) it gives the impression of unfairness or disrespect. Instead, the providers should change the attitude by providing effective remedies. This would raise trust and inspire customers to upload more data to the cloud, but then, also the data which was not transferred to the cloud before – sensitive data. This would be beneficial to both parties – a customer can use the service with some basic guarantees and the provider receives gain by addition of new customers (but risks with some number of litigations against them).

In the fourth chapter, the author turns to self-regulatory initiatives in cloud computing. The OECD Guidelines for Consumer Protection in the context of Electronic Commerce from 1999 already arrange for an electronic commerce system of transparency and predictability.\textsuperscript{17} It is driven by the idea that shopping

\textsuperscript{15} Article 6(1) of the Unfair Terms Directive (93/13/EEC).
\textsuperscript{16} Imbalanced T&Cs are seen as terms which only oblige one party of the contract (the customer) and try to exclude or mitigate any obligations on the part of the service provider. Balanced T&Cs provide both parties to the contract similar grounds to enforce their rights under the contract.
online should no less protected as purchasing goods offline. Although these guidelines offer a very general approach, they still include the most important keywords, such as transparency, access to information and effective remedies.

Also, in the fourth chapter, Cloud Industry Forum’s Code of Practice (CIF’s CoP) – promoting itself as a guardian of transparency – is analysed and CIF certified providers’ T&Cs are compared with the providers who are not in an attempt to draw conclusions about the efficacy of this initiative. As transparency is one of the important keywords of this thesis, it is necessary to see if CIF’s CoP truly provides an improved remedial situation for a cloud user.

The chapter also turns to other assurance seals provided by the Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) and TRUSTe. CSA STAR is a security assurance which also highlights the principle of transparency while TRUSTe is a privacy-related assurance which provides a negative example of a trust assurance.

The core idea to analyse soft-law initiatives is to see if these in fact help to provide transparency and fair contract terms to the customers. Signatories to the self-regulatory initiatives voluntarily undertake to use the certificates as a sign of quality (or may be seen as some sort of guarantee by the customers).

---

18 Ibid, “The Guidelines for Consumer Protection in the Context of Electronic Commerce, approved on 9 December 1999 by the OECD Council, are designed to help ensure that consumers are no less protected when shopping online than they are when they buy from their local store or order from a catalogue. By setting out the core characteristics of effective consumer protection for online business-to-consumer transactions, the guidelines are intended to help eliminate some of the uncertainties that both consumers and businesses encounter when buying and selling online.”
1.3 Significance

The thesis wishes to raise cloud providers’ attention to the fact that they can also profit from transparent contracts where the provider’s liability for every unwanted event is not excluded. The idea is to be “first in class”, provide something which other providers do not – some guarantee, responsibility and redress. The significance lies with this argument. As explained above, cloud computing industry will grow even more in the future. Awareness of data protection issues and other risks related to cloud computing by the consumers will also increase. The providers of today should address these issues already now.

Besides, providing remedial insights of the cloud providers’ T&Cs the thesis aims also to highlight the importance of actually reading the T&Cs and making a value judgment to accept or discard the standard form contract on that basis. At the same time, providers should not employ a business model where T&Cs with their length and complexity are designed to be left unread by their customers.

To sum up, the thesis will analyse the characteristics of cloud service contracts (Chapter 2), after which the service provider’s T&Cs will be analysed from a consumer protection prism and a lens of effectiveness (Chapter 3) and subsequently, the self-regulatory initiatives of cloud contracts will be assessed (Chapter 4).

---


2. Characteristics of a Cloud Contract

2.1 Cloud Computing

Cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

According to the National Institute of Standards and Technology (NIST), the “cloud” comprises of five essential characteristics, three service models and four deployment models.

Essential characteristics of the cloud are: a) on-demand self-service; b) broad network access; c) resource pooling; d) rapid elasticity; and e) measured service. To put it bluntly, cloud computing “consists” of a large number of computers connected through a real-time communication network such as the Internet. It means that if ten years ago a person or a company needed a physical storage device (e.g. server or a USB stick), now the service is provided by the cloud provider’s servers located world-wide, which makes it a “virtual” hardware for the user, because the users do not need to have a physical storage device for the backup. Users just need to have a Gmail account which provides the user with free storage space in Google Drive (similar system with Microsoft’s e-mail and OneDrive and different service providers).

22 Ibid, “A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.”
23 Ibid, “Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).”
24 Ibid, “The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.”
25 Ibid, “Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.”
26 Ibid, “Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.”
27 Due to trademark dispute, the name of SkyDrive changed to OneDrive. See <http://techcrunch.com/2014/02/19/microsoft-officially-rebrands-skydrive-to-onedrive/> accessed 9 May 2014.
NIST describes the three service models the thesis already mentioned above. These are:

- **Infrastructure as a Service (IaaS):** “The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).”

  For example, if a consumer opts to subscribe to Dropbox Pro, the user receives 100GB of storage space for $9.99 per month.

- **Platform as a Service (PaaS):** “The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.”

Examples of PaaS providers are Google Apps for Business, Amazon EC2 and Windows Azure.

PaaS and IaaS are referred to as utility computing services.

- **Software as a Service (SaaS):** “The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited

---

Salesforce.com’s CRM is a good example of SaaS service. SaaS runs on IaaS and/or PaaS and thus the cloud service platforms can be “stacked.”

According to NIST, the “cloud” comprises of four deployment models – private cloud, community cloud, public cloud and hybrid cloud. This thesis only focuses on the public cloud, which means that the cloud service is provisioned for open use by the general public. It is not tailor-made to meet a specific company’s needs and is made available in a pay-as-you-go manner.

Subsequently, this chapter will introduce some of the critical concepts of cloud contracts between a provider and a customer/consumer, viz. imbalance of negotiation powers (see 2.2 below), “click-through contracts” (see 2.3 below) and the notion of “vendor lock-in” (see 2.4 below). These notions are essential when analysing cloud contracts because they outline the imbalanced remedial situation when contracting online.

---

33 For example a SaaS provider may use the platform of Amazon EC2 (PaaS) to provide SaaS services.
2.2 Imbalance of Negotiation Powers

2.2.1 Standard term contracts – a feasible and balanced method of contracting at present day?

A balanced contract would mean that similar remedial possibilities are provided to both parties of the contract. Inequality of bargaining power together with the principle of freedom of contract implicates, however, imbalance. Furmston observes that this has led to a suggestion that contracts should be treated differently where there is inequality of bargaining power. Still, inequality itself cannot be a ground for invalidity. The process of mass production and distribution of goods and services which has supplemented individual effort has introduced the mass form of contracting – uniform agreements which must be accepted by all who contract with large-scale organisations. In the online context, this form of contracting entails even more serious difficulties – the parties do not physically meet and the contract is not “signed” with the signatures of the parties.

Looking the problem from a different angle, at present day it would be unimaginable if a person would need to go to a “local Google office” to conclude a cloud contract. This would involve too much costs and users who would be able to start using the service from home, would need to spend useless minutes or hours for concluding a contract which could be made easily via the customer’s own device far from the office. Arguably, online standard form contracts may be considered as a feasible solution for contracting.

Clearly, this view has its stumbling blocks and the situation is mutually beneficial only to an extent - if no errors occur and both parties duly perform their main obligations (customer pays and the provider delivers the service). A problem might befall if there is a situation that needs redressing (e.g. the provider does not keep the promised uptime) and/or the customer wants to withdraw the contract or demands compensation for harm done (e.g. data loss). In this case, for example, the customer may come to realise that the contract he or she has concluded does not provide the customer any refunds in case of termination or that there is a limited timeframe to initiate proceedings against the provider. These are the issues that customers usually

38 Ibid.
do not pay attention to prior entering into a contract, they come as a surprise later. Reason for this is that the T&Cs are overlong and difficult to understand for a layperson.

In the view of the author, the first step to become a truly feasible contracting solution, the T&Cs directed towards natural persons must be written in a plain, everyday language to be accessible to everybody. The T&Cs cannot be stacked – missing one hyperlink in the maze of the text consequently cannot lead to a situation where the user is unable to get acquainted to all of the contracting terms prior to concluding the contract. Such terms can be considered secret or at a minimum, hardly accessible and non-transparent.

Undoubtedly, there are always customers who will accept the T&Cs even knowing that the standard term contract includes imbalanced terms. Consumer protection law does not wish to remove such an option from the consumer and affect the autonomy of a person, rather, it caters to deliver a chance to those customers who are unaware that often the T&Cs are not transparent and include impediments to seek an effective remedy.

2.2.2 Who are influenced by the state of disequilibrium?

“Consumer” is any natural person who is acting for purposes which are outside his trade, business, craft or profession.\(^{39}\) An example of concluding a cloud contract is a situation where a natural person makes a personal e-mail account on Gmail and uses it for personal correspondence. This would be the most clear-cut situation. Unfortunately, this is often not the case and cloud services (e.g. in case of IaaS) are often for business (related to profession). Making a distinction when a user is “dealing as a consumer” is a difficult problem to comprehend. In the example above, if a self-employed person creates a Gmail account at his premises – is he making the email account for business-related activities or for private use? If he is making it for private use, consumer protection laws will apply and, thus, the user receives stronger protection. If not, the contract is the main source of “law” and the dispute will largely be settled on the basis of that contract. Clearly, there is a big difference in the outcome, provided that T&Cs often include the “whole agreement” clauses which are inserted to the contracts that courts would interpret the contract

\(^{39}\) Article 2(1) of the EU directive 2011/83/EC on consumer rights.
according to its “plain word meaning.” The problem is that law makes the assumption that it is easy to differentiate private and business use, while in practice it is not. It is also clear that the only situation when it is possible to decide whether a cloud contract has been concluded for private or business use is the moment of “signing.” Otherwise, during the usage of the cloud service, the determination becomes almost impossible. If a contract has a dual purpose, recital 17 of the Directive 2011/83/EC prescribes that a person should be considered a consumer, when the contract is concluded for purposes partly within and partly outside the person’s trade and the trade purpose is so limited as not to be predominant in the overall in the overall context.

Also, SMEs are not devoid from protection of unfair terms. This is practical because SMEs usually are in a situation where they cannot negotiate the contract terms and also need protection from clearly unfair terms. Still, it is clear that businesses receive a lesser degree of protection, and, under UK law, only particularly severe terms in B2B contracts can be considered unfair.

---

43 See Kingsway Hall Hotel Ltd v Red Sky IT (Hounslow) Ltd [2010] EWHC 965 (TCC) where the claimant argued that in a B2B contract, the liability exclusion clause was unfair. The Court held that: “In any event, for the reasons set out above, the Unfair Contract Terms Act section 11 applies. The terms following which restricted liability were unreasonable to be included having regard to the circumstances which were or reasonably ought to have been known to Red Sky or Kingsway, or be in the contemplation of the parties when the contract was made.” Under Estonian law (civil law), the Supreme Court of the Republic of Estonia has provided a judgement (Case No 3-2-1-88-04, paragraph 13) which clearly stipulates that terms in B2B contracts may also be unfair (and thus void under Estonian law), but this premise is rebuttable. Further analysed under section 3.4.
2.3 “Click-Through/Click-Wrap Contracts”

Cloud contracts are “click-through contracts” – electronic agreements where the T&Cs of the agreement are located on the same page as the “I agree” button. The T&Cs with their mean length and legalese are difficult to comprehend for a layperson. Stemming from this, nobody actually takes the effort to read through the contract terms. Thus, consumers are very often contracting without actually knowing what are they “signing.”

Why? It is fair to suggest that this problem occurs because cloud contracts are also “take it or leave it” (TIOLI) contracts – even if consumers would read the terms, they cannot affect their existence or form anyhow. The consumer or a SME is proposed with a standard contract from the provider and the weaker party is left with a choice – to agree with the terms of the contract and use the service, or disagree, and subsequently lose the chance to use the service. There might be also an issue of excessive trust placed in the service providers by the consumers and thus the standard term contract is left unread. Some consumers might not even comprehend that the simple box-ticking is actually a legally binding agreement.

Raising awareness and transparency is important, but on the other hand consumers do not want fifteen page-long T&Cs. There must be a middle way. The compromise must not be made by neglecting important terms but by making easily understandable terms (Dropbox might be a role-figure).

What if people knew all the terms and legal implications arising from the T&Cs? Would this make people to turn from Amazon, Google, Microsoft and the other? Probably not, because the technology itself is too tempting and simplifies our communication with others to such an extent that people are willing to sign these contracts anyway.

Adam Gatt raised the debate whether consumers really understand the implications of a mouse-click while contracting online already in 2002. Commencing a survey with 502 participants, his study showed that most of the participants were not aware that they were entering into a legally binding agreement when clicking “I agree” to the T&Cs. This is worrying while taking into account the fact that click-wrap
contracts have become a ubiquitous form of contracting. Some more recent research shows that the situation has matured, but it is evident, that the percentage of consumers who comprehend these complex T&Cs is speculative.

As mentioned above, the main difference between a click-wrap and an offline contracts is that no negotiations are held online and the contract is not a result of bargaining. The click-wrap agreements are concluded without the contracting parties never physically meeting one another. There is no physical signature under the contract as well. The mouse-click has taken the form of signature and courts have upheld this form of conducting business.

Click-through contracts are seen as easy, cheap and an effective way of promoting economic efficiency. They also reduce transaction costs and allow vendors (from SMEs to large corporations) to sell more goods and services. It must be remembered that click-wrap agreements still need to take into account principles of contract law to be enforceable – this means that the offer and acceptance have to be (legally) exchanged and the terms must be presented to the consumer prior to accepting (clicking “I agree” with the T&Cs). If the consent has not been given legally or if the terms are unfair, the click-wrap agreement is still unenforceable. Author agrees to the opinion that click-wrap agreements are a feasible way of contracting online, but the worrisome fact remains that people do not give their informed consent when concluding these contracts. Obviously, the contract cannot be unenforceable because the customer did not take the time to read the contract, but if these contracts are meant to be concluded, so to say, blind-folded, such an economic approach is not completely moral. Thus, I agree to an extent with Techliberation.com’s and Ars Technica’s journalist Tim Lee who opposes the view of click-wrap agreements

49 A. Gatt, “Electronic Commerce – Click-Wrap Agreements: The Enforceability of Click/Wrap Agreements”, p 407.
being an easy and an effective means of contracting. He sees click-wrap agreements as impediments to economic efficiency. Lee claims that if the society allows extremely cheap contract formation to one of the party (cheap in terms of the amount of people it is presented with) while the other party has to spend a lot of effort to scrutinize the offer will lead to too much taxpayer money being wasted on contract litigation.\textsuperscript{50} Author agrees that “promoting the economic efficiency” is a term disguised to mean profit for the service providers, not necessarily to the customers if the performance of a contract encounters problems and seeking a remedy becomes a necessity for a customer.

2.4 “Vendor Lock-in”

“Lock-in” issue concerns both the consumers and SMEs. Both of them may become dependent on a vendor’s cloud services. Customer “lock-in” means that the party is unable to use another provider without substantial switching costs. All of the bigger cloud providers (Microsoft, Google and Amazon) try to lock in the customer with one or more ways. Mostly the providers try to make a platform where it is possible to do several things conveniently together – create, save, edit and share – without paying for different applications. This is done with APIs. These APIs determine how some software components interact with others (like Gmail and Google Drive). As Armbrust et al. point out, these APIs are largely still proprietary (not open source) and therefore subscribers cannot migrate their data from one service provider to another.

M. Mowbray points out that “lock-in” may occur in different layers: a consumer or a SME might find it difficult to change their cloud infrastructure provider and also difficult to change their provider of cloud-based software for managing marketing campaigns (does not concern consumers).

European Union Agency for Network and Information Security (ENISA) lists “lock-in” as one of the security risk related to cloud computing.

---

2.5 Characteristics of a Cloud Contract - Findings

The second chapter gave the reader an overview about the essence of the “cloud.” It introduced the five essential characteristics, three service models and briefly listed the four deployment models. The thesis will analyse the public cloud of three service models – IaaS, PaaS and SaaS. Cloud providers use standard term contracts for concluding the service contract with consumers and SMEs.

Clearly, consumers and SMEs do not possess similar negotiation powers as the large cloud service providers. Inequality of bargaining power implicates that click-wrap agreements are offered to the customers on a take-it-or-leave-it basis. This means that the remedial situation cannot be evenly balanced from the start. Being a convenient form of contracting to a large number of people for the enterprises, the feasibility of such a form of contracting is extremely doubtful if the business model is built on the premise that customers will not delve into the T&Cs of these cloud services anyway. In such a case, the remedial situation is most likely to be poorly designed and risks in the contracts are badly divided – the service provider has mitigated and/or excluded as much risks as possible while the customer is not equipped with similar tools under the contract. Thus, standard terms provoke massive inequality. The standard form contracts would be a feasible method of contracting only if the providers would not abuse their negotiation powers as they do today.

The “lock-in” issue only exacerbates the issue of poor remedial situation to the detriment of the customer. It is designed to keep the customer locked with the provider through APIs – by making the services appealing to the customer by their compatibility with different service products.

In total, the characteristics of the cloud contract implicate that the starting line of the parties to a cloud contract is not in the same place and the remedial situation might be imbalanced. Next, the author turns to the T&Cs of the six cloud service providers to see, if such an insinuation can be affirmed or inverted.
3. **Analysing the Cloud Contract’s Terms and Conditions in the Light of Consumer Law**

This chapter analyses the T&Cs of six cloud providers (see 3.3 below) from the prism of consumer protection and from the criteria of effectiveness. Consumers receive a higher level of protection, because the assumption is made that they are the weaker parties of the contract due to lack of bargaining power and, as the freedom of contract principle allows drafting of too unbalanced T&Cs, the protection conferred is necessary. The scope of the enquiry is to analyse the remedies from the criteria of effectiveness which works as a negative test – if none of the barriers exist, the remedial situation can be considered a balanced one.

Community law prescribes rules about unfair terms in consumer contracts (93/13/EEC) which will be the grounding legislation for analysing clauses in the cloud providers’ standard T&Cs. It protects consumers as weaker parties against the suppliers and provides that unfair terms are not binding to the consumer. Directive 2005/29/EC protects consumers against unfair commercial practices, which are prohibited under this Directive. Directive 2000/31/EC (the E-Commerce Directive) applies to information society service providers and sets information requirements (transparency!) also for cloud service providers to abide by prior to contracting online. The newest piece of legislation is the Directive 2011/83/EC – the Consumer Rights Directive – which applies to distance contracts between a consumer and a trader.

Firstly, the chapter turns to the term “consumer” and undertakes to give underlying reasons for consumer protection in the society. Secondly, the author analyses the abovementioned consumer protection directives. Thirdly, analysis on the terms and conditions of six cloud service providers is given. Fourthly, the chapter provides the overview of the relevant consumer protection laws of the United Kingdom and Estonia. The comparative part highlights the different policy decisions towards the protection of SMEs who suffer similarly from unfair terms in the standard form contracts. Lastly, the author gives an overview of the findings and gives opinion about the remedial situation in the cloud contracts.
3.1 Definitions of a “Consumer” and an “Average Consumer”

Definition of a “consumer” has been a debated one, although staying essentially the same throughout the last two decades. In the Directive 93/13/EEC, a consumer is defined in article 2(b) as any natural person who … is acting for purposes which are outside his trade, business or profession. Article 2(1) of Directive 2011/83/EC augments “craft” to the list mentioned above. Although explicitly set down in the Directives, the Court of Justice of the European Union (CJEU) in Idealservice had to answer the question whether a company may be regarded as a consumer. Court, being very explicit, said that article 2(b) of 93/13/EEC refers solely to natural persons. Therefore, it is not correct to state, that self-employed persons and companies (being a micro-, small-, or medium-sized enterprises) can be interpreted as being a consumer. However, the question here is not whether it is possible to fit a company under the definition of a “consumer” but whether the rationale to protect businesses is alike to the protection of consumers or not. This will be analysed subsequently.

Several Community directives make note of an “average consumer.” According to recital 18 of Directive 2005/29/EC, an average consumer is “…reasonably well-informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors…” Average consumer is a benchmark also for cloud contracting. He is a person who is interested in the remedial situation and is aware that cloud providers have access to customer’s data, also the underlying risks of this fact.

A more difficult question arises with the topic of businesses “dealing as a consumer”, a notion introduced in UK law. Cunningham and Reed propose that this situation is only occurring where a business is procuring cloud services for a private purpose. Cunningham and Reed bring front an UK case of R & B Customs

---

56 Commission Recommendation 2003/361/EC describe an “enterprise” as any entity engaged in an economic activity, irrespective of its legal form. This includes, in particular, self-employed persons and family businesses engaged in craft or other activities, and partnerships or associations regularly engaged in an economic activity (art 1).

57 Joined cases 541/99 and 542/99 Cape Snc v Idealservice Srl and Idealservice MN RE Sas v OMAI Srl, [2001], paras 10, 12-17.

Brokers Ltd v United Dominions Trust Ltd\(^{59}\) where the court upheld that in a situation where a company is acting as purchaser of goods or services, and if those goods or services are not bought as an integral part of the business, the company may be acting as a consumer.\(^{60}\) Clearly, this approach is very limited\(^{61}\) and does not include a situation where a microenterprise\(^{62}\) is contracting with Amazon or Google e.g. and has to face the same asymmetric situation as the consumer. Such a contract should be considered as being a B2C contract according to the recital 17 of 2011/83/EC\(^{63}\) and this is a clear example of \textit{de jure} company acting \textit{de facto} as a consumer, because the private use is predominant to the business-use.

3.1.1 \textbf{Rationale on consumer protection}

Why do we need to protect the consumers? What is the justification for this? Micklitz et al. state that the authorisation for a policy intervention can be found in the asymmetry of economic powers which is possible due to the principle of freedom of contract.\(^{64}\) The principle of freedom of contract allows one party of the contract to make pre-formulated contracts which are not negotiated and, thus, save a huge amount of money on transaction costs while the other party (and the public) are not necessarily benefitting from the same phenomenon. Standard terms do not share the guarantee of contractual fairness which according to the liberal doctrine characterises freely negotiated contracts based on self-determination.\(^{65}\)

According to Iain Ramsay, psychological experiments show that individuals care about how others are treated in the market and are willing to punish enterprises that act unfairly.\(^{66}\) The classical rationale of “inequality of bargaining power” emerges

\(^{59}\) [1988] 1 WLR 321. The decision has also received criticism, see M.P. Furmston, “Law of Contract”, p 239.

\(^{60}\) Upheld in a Court of Appeal decision Feldarol Foundry Plc v Hermes Leasing (London) Ltd. [2004] EWCA Civ 747.

\(^{61}\) Cunningham and Reed point out that an obvious example is where a micro-business run by a private individual signs up for a Gmail account to use it for personal correspondence, but uses this also for business purposes occasionally. See “Caveat Consumer? – Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud”, p 19.

\(^{62}\) According to art 2(3) of Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, a microenterprise is an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

\(^{63}\) “A person should be considered as a consumer, when the contract is concluded for purposes partly within and partly outside the person’s trade and the trade purpose is so limited as not to be predominant in the overall context”


\(^{65}\) Ibid.

already in the work of F. Kessler. The classical view highlights that the review of unfair terms is a form of weaker party protection and is meant to compensate somehow for unequal bargaining.

The classical view of consumer protection is also taken up by CJEU. In *Oceano*, CJEU clearly stated that “the system of protection introduced by the Directive [93/13/EEC] is based on the idea that the consumer is in a weak position vis-á-vis the seller or supplier, as regards both his bargaining power and his level of knowledge.

M. Hesselink encapsulates many underlining rationales for consumer protection. One is distributive justice. Arguably, contract law, in particular, protection against unfair terms contribute to a fairer distribution of resources between rich and poor. The other possible rationale against unfair terms is paternalism. It roots from the German idea that the default rule that would have applied in the absence of the contract term under consideration should be used as a yardstick for the fairness of the term: a term strongly deviating from this default rule is considered unfair.

---

69 Joined cases 240/98 to 244/98 *Océano Grupo Editorial SA v Roció Murciano Quintero* and *Salvat Editores SA v José M. Sánchez Alcón Prades*, *José Luis Copano Badillo*, *Mohammed Berroane* and *Emilio Viñas Feliú*, [2000], para 25.
70 M. Hesselink argues that this explanation is flawed in two ways: a) if the abuse of bargaining power is the problem, then it is not clear why price and other core terms should be excluded from the review (See art 4(2) of 93/13/EEC) and b) the weaker party hypothesis is empirically doubtful. See Hesselink “Unfair Terms in Contracts between Businesses”, p. 3.
71 Ibid., p 4.
72 Section 307 of the German Civil Code (BGB):
Test of reasonableness of contents: (1) Provisions in standard business terms are ineffective if, contrary to the requirement of good faith, they unreasonably disadvantage the other party to the contract with the user. An unreasonable disadvantage may also arise from the provision not being clear and comprehensible.
(2) An unreasonable disadvantage is, in case of doubt, to be assumed to exist if a provision
1. is not compatible with essential principles of the statutory provision from which it deviates, or
2. limits essential rights or duties inherent in the nature of the contract to such an extent that attainment of the purpose of the contract is jeopardised.
(3)Subsections (1) and (2) above, and sections 308 and 309 apply only to provisions in standard business terms on the basis of which arrangements derogating from legal provisions, or arrangements supplementing those legal provisions, are agreed. Other provisions may be ineffective under subsection (1) sentence 2 above, in conjunction with subsection (1) sentence 1 above.
Hesselink points out that this line of thinking was set by the CJEU in *Freiburger*\(^{73}\) when the Court stated that it is for the national court to decide, whether a contractual term is unfair in the sense of the Directive 93/13/EEC. This view is paternalistic, because the decision of unfairness is given to a Court, interpreting the intent of a legislator, prescribing what is in the best interest of the parties.\(^{74}\) Paternalism is a strong step in diminishing parties’ choices which is not a desired goal in contract law in general.\(^{75}\)

### 3.1.2 Rationale to (or not to) protect businesses against unfair terms

Thinking about the rationale in consumer protection leads us to the question, why only consumers? Do not the businesses suffer from the same kind of problems than consumers? If to be keen on protecting natural persons, why should not the same rationale hold for microenterprises (some cases maybe even small enterprises) that face the same problems as consumers – asymmetric information, imbalance of negotiation power, take-it-or-leave-it contracts? This is not only a problem of consumers and if unequal bargaining power is seen as a problem, then businesses can also be “in a weak position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge.”\(^{76}\) This is not a new idea and author believes that the same rationale holds for businesses similarly as to consumers. If imbalance of power is a problem in a B2C contract, it is no less so in a B2B agreement.\(^{77}\) This line of thinking has emerged, e.g. in Estonian law.\(^{78}\)

---

\(^{73}\) Case 237/02 *Freiburger Kommunalbauten GmbH Baugesellschaft & Co. KG v Ludger Hofstetter and Ulrike Hofstetter*, [2004], para 21.

\(^{74}\) In this sense, parties could overrule the legislator’s idea by making a negotiated contract.

\(^{75}\) M. Hesselink, “Unfair Terms in Contracts between Businesses”, p 9.

\(^{76}\) Joined cases 240/98 to 244/98, para 25.

\(^{77}\) M. Hesselink, “Unfair Terms in Contracts between Businesses”, p 4.

\(^{78}\) See section 3.4.
3.2 Relevant Directives for Cloud Contracting


3.2.1 The Unfair Terms Directive – 93/13/EEC (UTD)\(^{79}\)

Council Directive 93/13/EEC from April 5 1993 on unfair terms in consumer contracts is an instrument to strike down terms from B2C contracts when the term is considered unfair. It is a minimum harmonisation directive.\(^{80}\) Under this sub-section, the requirements and the consequences of the Unfair Terms Directive (UTD) are analysed.

The first and obvious requirement to apply the UTD is that it is a B2C contract – meaning that one party to the contract is a consumer\(^{81}\) and the other is a seller or supplier.\(^{82}\)

Secondly, it has to be identified whether the terms are “individually negotiated” or not\(^{83}\) to conclude if a term in a contract is a standard term or not. The term is considered to be a standard term if it is not being individually negotiated, if it has been drafted in advance and the consumer has not therefore been able to influence the substance of the term.\(^{84}\) Party claiming that the terms were individually negotiated bears the burden to prove this fact.

Before analysing if a certain term might be unfair, it is necessary to examine the exemptions of the UTD. The first exemption is laid down in article 1(2) of UTD. It

---

\(^{79}\) This sub-section has used its basis from C. Ginter, “Tüüptingimustest VÕS ja direktiivis 93/13/EMÜ.” Juridica 2001 No II. Available at <http://juridica.ee/juridica_et.php?document=et/articles/2001/7/6620.SUM.php> p 501-513.

\(^{80}\) Article 8 of 93/13/EEC provides that Member States may adopt more stringent provisions compatible with the Directive to ensure a maximum level of protection to the consumers. This brings about another problem, if Member States are allowed to make more stringent provisions; the level of protection varies in different Member States.

\(^{81}\) Article 2(b) of the UTD.

\(^{82}\) According article 2(c) of the UTD, a supplier is “any natural or legal person who … is acting for purposes relating to his trade, business or profession, whether publicly or privately owned.”

\(^{83}\) Article 3(1) of the UTD.

\(^{84}\) Article 3(2) of the UTD.
excludes from its scope terms that are reflecting the “mandatory statutory or regulatory provisions.” These are terms that parties cannot deviate from, e.g. parties cannot agree in a sales contract that the other party has one day to withdraw from the contract when by law he has 14 days.

The second exemption is laid down in article 4(2) of the UTD which excludes terms relating to the “main subject matter of the contract” and “the adequacy of the price and remuneration”. According to recital 19 of the UTD, this means that the quality/price ratio of the goods or services cannot be assessed when deciding whether a term is unfair or not.85

Last step is the “decision-making” – after making sure that the term does not fall under any of the aforementioned exceptions, the question turns to the fact whether the seller (or service provider) has abused his bargaining position by imposing unfair terms. For this, two tools exist: one under article 3(1) of the UTD and the other under article 3(3) of the UTD (see 3.2.1.1 below).

3.2.1.1 Material unfairness

The main rule is set in article 3(1) of the UTD, declaring that “a contractual term which has not been individually negotiated shall be regarded as unfair 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.” By reversing this term, the recipe for a fair term is provided – a term that is in accordance with the principle of good faith and does not impose conditions misbalancing the rights and obligations disadvantaging the consumer. Unfair terms do not bind the consumer.86 The word “significant” carries substantial weight in article 3(1) and implies that “trivial” imbalance caused by a standard terms cannot be considered unfair.

Article 3(3) refers to Annex I of the UTD which includes “an indicative and non-exhaustive list of the terms which may be regarded as unfair.”87 Annex I includes 17 instructive examples of unfair terms. It is a grey list of unfair terms88, meaning that

85 Very arguable approach, because imposing a price which is too high (compared to the quality of the good or service) can be considered unfair.
86 Article 6(1) of the UTD.
87 Article 3(3) of the UTD.
88 Recital 17 of the UTD provides that “the annexed list of terms can be of indicative value only…”
these terms are assumed to be unfair by law, but being a conjecture, this premise can be rebutted by the service provider – stating that (under article 3(1)) the term is “fair.” This also means that courts have discretion to decide that a standard term is not unfair, even if it is included in the grey list of Annex I.89

Article 4 of the UTD gives indications what factors should be included in the “decision-making.” Article 4(1) provides that the unfairness of a contractual terms shall be assessed, taking into account “the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract which it is dependent.” In essence, it provides that all circumstances and factors of the contract and the service have to be taken into account while deciding on the issue of unfairness.

In a CJEU case Freiburger Kommunalbauten90, the question arose which court should adjudicate the question of unfairness – CJEU or the national court? The question became relevant because in Oceano, the CJEU had adjudicated the issue and held that a term drafted in advance by the seller, the purpose of which is to confer jurisdiction in respect of all disputes arising under the contract on the court in the territorial jurisdiction of which the seller has his principal place of business, satisfies all the criteria necessary for it to be judged unfair for the purposes of the Directive [93/13/EEC]. CJEU in Freiburger made a rather vague distinction between the two cases91 and decided not to judge on the unfairness issue and hand it to the national courts to decide. In a nutshell, the Freiburger case involved two consumers who contracted with a municipal construction company who sold a parking lot to the two consumers in a car park that a construction company was to build. The price was due upon delivery of a security by the contractor, in case of late payment; the purchasers were liable to pay default interest. The consumers refused to pay the price before having accepted the parking space free of defects. The municipal construction company claimed default interest for late payment.

89 C. Ginter, “Tüüptingimustest VÕS ja direkteivis 93/13/EMÜ”, p 506.
90 Case 237/02, para 23.
Making a distinction between the two cases, CJEU in Freiburger stated “that assessment [of Oceano] was reached in relation to a term which was solely to the benefit of the seller and contained no benefit in return for the consumer.” Court went on to say that “whatever the nature of the contract, it thereby undermined the effectiveness of the legal protection of the rights which the [Unfair Terms] Directive affords to the consumer. It was thus possible to hold that the term was unfair without having to consider all the circumstances in which the contract was concluded and without having to assess the advantages and disadvantages that the term would have under the national law applicable to the contract.”92 Court concluded by saying that the same situation does not apply to the term at issue in Freiburger and it is for the national court to decide whether a contractual term … to be regarded as unfair under article 3(1) of the Directive 93/13/EEC.93 Consequently, after the Freiburger case, the national courts decide upon the (un)fairness of standard terms.

3.2.1.2 Unfairness in the formal sense

Article 5 of the UTD highlights that the terms drawn up in writing must always be drafted in plain, intelligible language. It provides an important guideline for this thesis, because it offers a chance to distinguish “fairness” under another aspect - besides the material sense, also in the formal sense. Thus, transparency is the most important aspect of the criteria of effectiveness.

In Cofinoga94 the CJEU delivered the twofold function of the transparency principle. Firstly, information provided by the service provider enables the consumer to compare offers (of different cloud providers) and secondly, it enables the consumer to assess the extent of his liability. Information has to be provided to the consumer prior to contracting.95 If the transparency principle is not followed, this is definitely to the detriment to the consumer because the consumer has to initiate proceedings against the service provider to seek “unfairness” in a competent court.

92 Ibid.
93 Ibid. paragraph 26.
95 Case 144/99 Commission of the European Communities v Kingdom of the Netherlands, [2001], Opinion of AG Tizzano, para 31.
Advocate General Tizzano stated in *Commission v Netherlands* \(^{96}\) – later fully relied upon in the judgement – that the supplier or seller is obligated to foresee from the start that clauses of the contract are drafted in plain and intelligible language.\(^{97}\)

According to Micklitz et al, the principle of transparency enshrined in article 5 of the UTD is a sub-category of good faith through the principle of legitimate expectations. Article 5 provides two standards – plainness and intelligibility - which are to be assessed differently.\(^{98}\) “Plainness” refers to the legal effect of a term, including its consequences. It roots from the idea that a consumer needs to know what to expect (remember *Cofinoga!*\(^{99}\)) from the contract. Ambiguous formulations should not put the seller or supplier in a situation to improve his legal position at the consumer’s expense. “Intelligibility” refers to legibility. It seeks to eliminate the so called “small print” from the T&Cs which the consumers find readily difficult to comprehend. In total, the seller or supplier must draft the standard terms plainly from an editing and optical point of view. The requirement of intelligibility also entails a qualitative element – requirement for information.\(^{99}\) The terms must not mislead the consumer about the scope of his rights and obligations.\(^{100}\)

To transpose this into the contracting situation, it means that a consumer is to be placed in a position where he can assess his legal position with the help of the information provided by the service provider in order to make a decision on the conclusion of the contract or to assess the risk of a possible withdrawal from the contract. According to Micklitz et al, the principle of transparency also contains a competitive function: the consumer needs to be in a situation to decide whether or not to enter into a more advantageous contract. This approach was employed by the CJEU in *Cofinoga*, where the Court explicitly recognised the twofold function of the transparency principle.

Although the UTD will be the most important instrument that will be further analysed in the thesis when focusing on the validity of the standard terms, the

---

96 Case 144/99 *Commission of the European Communities v Kingdom of the Netherlands*, [2001], para 20.
98 Ibid.
99 “Intelligibility” also includes the linguistic element in order to attain the protective ambit of the Directive. See H.-W. Micklitz et al. “Understanding EU Consumer Law”, p 136-137
100 Ibid.
author wishes to make note of other relevant Community law in the context of cloud contracting.

3.2.2 **Directive 2005/29/EC concerning unfair B2C commercial practices (UCP).**

UCP is aimed at protecting consumers from unfair commercial practices which, according to article 2(d), refers to “any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers.” Unfair commercial practices are prohibited under art 5(1) of the UCP and a commercial practice is unfair, if it is contrary to the requirements of professional diligence and it materially distorts or is likely to distort the economic behaviour with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers (article 5(2) (a) and (b)). Annex I of the UCP contains a blacklist of commercial practices which are to be considered unfair in all circumstance, e.g. where the trader claims to be a signatory to a code of conduct when he actually is not.

3.2.3 **Directive 2011/83/EC, Consumer Rights Directive (CRD)**

As the cloud contract is usually a distance contract, the CRD applies to a B2C cloud contract.101

Consumer Rights Directive is applicable to any distance contracts concluded between a consumer and a trader.102 Thus, if a consumer is located in the EU, the CRD applies. For the purposes of this thesis, further analysis is made only on article 6 which prescribes the pre-contractual information obligations the trader must provide to the consumer. Information provided must be clear and comprehensible according to article 6(1) of the CRD. Again, reference to the principle of transparency is made. Article 6(1) delivers a rather extensive list of compulsory information set which has to be communicated to the consumer to meet the transparency principle. These include: a) the main characteristics of the goods or

---

101 “Distance contract” means any contract concluded between the trader and the consumer under an organized distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded (Art 2(7)).

102 Article 1 of the CRD.
services, to the extent appropriate to the medium and to the goods or services; e) total price of the ... services inclusive of taxes, or where the nature of the ... services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated ...; h) where the right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with article 11(1), as well as the model withdrawal form set out in Annex I(B); n) the existence of relevant codes of conduct, as defined in point (f) of article 2 Directive 2005/29/EC ...; r) ... the functionality, including applicable technical protection measures, of digital content. If any of the rights provided to consumers under the CRD are waived or restricted by a contractual term, they are considered not to bind the consumer under article 25 of the CRD. This approach mirrors article 1(2) of the UTD, providing mandatory rules which parties cannot deviate from.

3.2.4 **Directive 2000/31/EC – on electronic commerce (ECD)**

ECD applies to information society service providers. Recital 17 of the ECD provides that the definition of “information society service” covers “…any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service...” Cloud service covers these four requirements and this implies that the cloud service provider is an information society service provider and, thus, initiates the applicability of the ECD.

Article 5(1) of the ECD (see also recital 12 of the CRD) provides that in addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients...at least the following information: a) name of the service provider; b) address of the service provides; c) registration number of the service provider; e) supervisory authority if the activity of the service provider is subject to an authorisation scheme; f)VAT number. Article 5(2) provides that where the information society services refer to prices, these must be indicated clearly and unambiguously and … indicate whether they are inclusive of tax and delivery costs.

Under article 10, this information requirement is complemented with a rule that different technical steps to follow to conclude the contract must be clearly and
unambiguously provided to the customer. Again, as the CRD, the ECD prescribes service providers to give information about the identity of the provider. Similarly, it can be seen as a transparency tool and facilitator of trust in electronic commerce.
3.3 Analysis on the Terms and Conditions

This section aspires to analyse the standard terms of six cloud service providers: Dropbox and UKFast; Google Apps for Business and Windows Azure; Salesforce.com and Dell Boomi. The analysis divides the cloud offering models – IaaS, PaaS and SaaS providers will be analysed separately. Thus, IaaS providers will be compared with each other and so on. The analysis will not make specific comparisons between, e.g. IaaS and SaaS providers, but will only provide generalised remarks in 3.6 below. T&Cs will be analysed through the lens of the four criteria of effectiveness (four barriers to an effective remedy) and consumer protection laws(s). The four criteria – transparency, time, costs and clear-cut cases of abuse of bargaining power – provide indications on the remedial situation offered by the cloud service providers in their T&Cs. If the standard terms do not infringe any of the four criteria, the remedial situation is considered balanced under the analysis. On the contrary, if the T&Cs infringe any of the criteria, it means that a service provider is imposing barriers to seek an effective remedy and, thus, the remedial situation is imbalanced.

The “transparency” criteria will focus on hidden terms, termination and whole agreement clauses. “Time” refers to limits set to initiate proceedings. “Costs” relate to termination (refunds) and jurisdiction clauses. “Clear-cut cases of abuse” provide general indications about the inequality of the contracting situation. Examples of such cases would be modification and variation clauses, assignment clauses and clauses which transfer the provider’s obligations to the customer. The analysis will only make note of standard terms infringing these criteria. Thus, no good examples of balanced contract terms will be provided. Assessing the remedial situation under these criteria of effectiveness enables the author to give clear indications about the (im)balanced contracting situation.

Subsequently, sub-section 3.3.1 analyses the T&Cs of IaaS service providers (Dropbox and UKFast); sub-section 3.3.2 examines the T&Cs of PaaS providers

---

103 Terms were analysed between 17th of February until 28th of February. Note that from 24 of March 2014, Dropbox has renewed its Terms of Service and Privacy Policy. Consequently, the thesis makes note if the latest version of the terms deviates from the older version under analysis. In total, it must be stated that the changes are rather cosmetical.
(Google Apps for Business and Windows Azure) and sub-section 3.3.3 SaaS providers (Salesforce.com and Dell Boomi) respectively.

3.3.1 **Infrastructure as a Service platform providers – Dropbox and UKFast**

3.3.1.1 Dropbox

3.3.1.1.1 **Transparency and Costs – Termination**

Transparency is one of the most important aspects of seeking an effective remedy. As provided by the CJEU, the principle of transparency allows the consumer to compare different offers and assess the extent of his liability.\(^{104}\) In case of Dropbox, the lack of transparency occurs with the termination clause. Termination clause of Dropbox is provided in the Acceptable Use Policy (AUP) under “Termination” and under the Pricing Terms and Conditions (PTCs) “Cancelling Your Account.”\(^{105}\) This already shows that getting a clear overview of the termination procedure, the customer has to go through two different policies. This violates the principle of transparency, specifically the intelligibility requirement due to the fact that it misleads the consumer about the full extent of his right of withdrawal under the contract. “Termination” of the Dropbox’s T&Cs stipulates that “though we’d much rather you stay; you can stop using our Services any time. We reserve the right to suspend or end the Services at any time, with or without cause, and with or without notice …“\(^{106}\) Consequently, the customer is allowed to terminate any time he or she wishes and Dropbox does not prescribe any formal requirements for termination. However, the PTC “Cancelling Your Account” provides that “Dropbox Premium Accounts are prepaid and are non-refundable. Dropbox does not provide refunds or credits for any partial months or years. You may cancel your Dropbox Premium Account at any time, and cancellation will be effective immediately.” In total, it must be stated that the Dropbox’s termination clause infringes article 5 of the UTD (the transparency requirement) because the termination clause is divided into two different policies and the “Termination” clause does not provide any reference to the “Cancelling Your Account” clause in the PTCs, thus, the customer is provided with insufficient information for termination. Similarly, barriers are set in the form

\(^{104}\) See [*supra* note 94].

\(^{105}\) Dropbox does not use numerical classification of terms.

\(^{106}\) In the latest version of Dropbox’s ToS there is no separate policy for PTC and the rule that no refunds are provided is set in the ToS (Under “Paid Accounts”). Thus, the consumer does not have to browse to separate policies at present.
of costs of termination. If no refunds are provided, it unquestionably undermines the
notion of “terminating at any time”, conversely, the customer has to be very specific
on the dates when to terminate and, therefore, is forced to be locked in to the service
more than the customer may want.

3.3.1.1.2 Costs – Jurisdiction clauses
Costs are also affected with the jurisdiction clauses. Dropbox’s jurisdiction clause
confers jurisdiction in the U.S, in California.\textsuperscript{107} If a European consumer should go
to court in the U.S, it would be the biggest obstacle to seek redress. Fortunately, the
consumer protection laws of Europe shield the consumer against such cases.
Conferring jurisdiction away from the home state of the consumer may hinder “the
consumer’s right to take legal action or exercise any other legal remedy” under sub-
indent (q) of Annex I of the UTD. Especially litigation outside Europe is a barrier to
seek redress for consumers and SMEs. As CJEU put it in \textit{Oceano}\textsuperscript{108} a term, which
confers jurisdiction in respect of all disputes arising under the contract on the court
in the territorial jurisdiction of which the seller or supplier has his principal place of
business and obliges the consumer to submit to the exclusive jurisdiction of a court
which may be a long way from his domicile may make it difficult for him to enter
an appearance. In the case of disputes concerning limited amounts of money, the
costs relating to the consumer's entering an appearance could be a deterrent and
cause him to forgo any legal remedy or defence. CJEU makes the obvious
conclusion that “such a term thus falls within the category of terms which have the
object or effect of excluding or hindering the consumer's right to take legal
action.”\textsuperscript{109} The CJEU in \textit{Oceano} found the standard term conferring jurisdiction
unfair.\textsuperscript{110}

\begin{footnotesize}
\textsuperscript{107} “Miscellaneous legal terms” provide that that “…the use of the services and software will be governed by
California law except for its conflicts of laws principles. All claims … must be litigated exclusively in the Federal
or State courts of San Francisco County, California, and both parties consent to venue and personal jurisdiction
there.” In the latest version (under “Controlling Law”), the ToS provide that “These Terms will be governed by
California law except for its conflicts of laws principles.”
\textsuperscript{108} Joined cases 240/98 to 244/98, para 22.
\textsuperscript{109} Ibid.
\textsuperscript{110} Joined cases 240/98 to 244/98, paras 15-16. The cases involved consumers who were residents of Spain and
entered into contract for the purchase by instalments of an encyclopaedia for personal use. The contracts contained
a term conferring jurisdiction on the courts in Barcelona, a City which none of the defendants in the main
proceedings is domiciled but where the plaintiffs in those proceedings have their principal place of business.
\end{footnotesize}
Under article 16(1) of the Council Regulation No 44/2001 (Brussels I Regulation), the consumer may initiate proceedings against the other party of the contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled. Under article 15(2) of the Brussels I Regulation, if the service providers is not domiciled in any of the Member States, but has a branch, agency or other establishments in one of the Member States, the provider is deemed to be domiciled in that State. Article 16(1) of the Brussels I Regulation allows the consumer to initiate proceedings in the court where he is domiciled. This does not yet answer where is the dispute settled when the consumer is sued under a contract that confers the jurisdiction to the courts of the U.S. Article 16(2) of the Brussels I Regulation provides that proceedings against a consumer may be brought by the service provider only in the courts of the Member State in which the consumer is domiciled. Consequently, the consumers cannot be sued elsewhere than in the Member State where the consumer is domiciled and any attempt to confer jurisdiction to a court where the consumer is not domiciled, is unfair under sub-indent (q) of Annex I of the UTD.

Article 6(1)(a) of the Regulation No 593/2008 (Rome I Regulation) provides that consumer contracts shall be governed by the law of the country where the consumer has his habitual residence and the professional (seller) pursues his commercial activities in the country where the consumer has his habitual residence. Therefore, consumers do not have to be concerned about the applicability of foreign law to solve disputes arising from the contract.

Such is the shield provided by the Community law to the consumers, who are considered as a weaker party to the contract. Nevertheless, SMEs cannot enjoy the same comforts and the courts of the Member States have to address if such clauses hinder seeking a remedy or if the parties are in a position to decide best where to solve the arising disputes. For example, under Estonian law, such jurisdiction and

112 Article 15(2) of the Brussels I Regulation.
governing law clauses in B2B contracts might be held to be unfair if they are seen as a barrier to seek a remedy (see 3.4.1 below).

3.3.1.1.3 Clear-cut case of abuse – Transferring the provider’s obligations to the customer

“Your Responsibilities” of the PTCs of Dropbox stipulate that “You, and not Dropbox, are responsible for maintaining and protecting all of your stuff. Dropbox will not be liable for any loss or corruption of your stuff, or for any costs or expenses associated with backing up or restoring any of your stuff.” This implies that when a customer of Dropbox uploads files to the cloud, it is the user who has to protect all the materials uploaded. Although Dropbox incites users to encrypt the files uploaded to the cloud, this clause seeks to exclude liability on the behalf of the service provider. Maintaining and being responsible for protecting all of the data uploaded is literally impossible and illogical because as described above, the cloud consists of interconnected servers in different locations of the world and the user has no access or control over them. This means that service provider’s obligations are transferred to the user and Dropbox uses such a term to exclude its liability for any interference with the “stuff” uploaded.

This term is conceivably unfair under sub-indent (o) of Annex I of the UTD as it obliges the user to fulfil all his obligations (pay for the service) where the seller must not perform his obligations under the contract – protect the uploaded files with reasonable care and skill.

3.3.1.1.4 Clear-cut case of abuse – Modification and variation

Firstly, the modification clause of Dropbox will be discussed. Under sub-indent (j) of Annex I of the UTD, a term in a standard contract can be considered unfair if it enables the service provider to alter the terms of the contract unilaterally without a valid reason which is specified in the contract. Sub-indent (j) foresees a transparent modification clause where the grounds for alterations are provided in the contract.

---

114 Under “How to Add Your Own Layer of Encryption to Dropbox” in the Security Overview provides: “Dropbox applies encryption to your files after they have been uploaded, and we manage the encryption keys. Users who wish to manage their own encryption keys can apply encryption before placing files in their Dropbox. Please note that if you encrypt files before uploading them, some features will not be available, such as creating public links. Doing so will also make it impossible for us to recover your data if you lose your encryption key”

115 Sub-indent (j) of Annex I of the UTD.
Dropbox’s modification clause (“Modifications”) provides that Dropbox may “… revise these Terms from time to time and the most current version will always be posted on our website. If a revision, in our sole discretion, is material we will notify you…. Other changes may be posted to our blog or terms page, so please check those pages regularly. By continuing to access or use the Services after revisions become effective, you agree to be bound by the revised Terms. If you do not agree to the new terms, please stop using the Services.” This is a problematic modification clause from many aspects. Firstly, the alteration is not linked to any grounds besides Dropbox’s own discretion. Secondly, the notifications are only provided to the user if they are “material.” Deciding what is “material”, is in the sole discretion of Dropbox. Therefore, a theoretical possibility stays that the contractual situation is changed to the detriment of the consumer by making several “small” changes which add up to a material change, but which need not then be notified under this clause.116 Thirdly, there exist some “other changes” that are posted to Dropbox’s blog or term page and the user himself must be active to be able to see the changes. This is against information requirements set in the ECD. The information provided to the user must be “easily, directly and permanently accessible” according to article 5(1) of the ECD. This means that the user should not be the one making the active effort to receive extra information about the contract. Fourthly, the arguable problem arises with the consent because there may be changes to the T&Cs that the customer never becomes aware of. As sub-indent (j) of Annex I of the UTD prescribes that the contract must give specific grounds for alterations and Dropbox has not provided any, the term can be considered unfair under sub-indent (j).

Secondly, the variation clause will be analysed. Sub-indent (k) of Annex I of the UTD foresees that a standard term is possibly unfair if it enables the service provider to alter unilaterally, without a valid reason, any characteristics of the service provided.117 Acceptable Use Policy (under “Termination”) stipulates that Dropbox “… may stop, suspend, or modify the Services at any time without prior notice to you. We may also remove any content from our Services at our discretion.” Clearly, this term does not provide any valid reasons for variation of the service

---

116 In the latest version, Dropbox has polished the “Modifications” term by rephrasing the term “materially” by constructing that if a “…revision meaningfully reduces your rights…” the user must be notified.
117 Sub-indent (k) of Annex I of the UTD.
besides Dropbox’s own discretion. This is a sign of abuse of the superior negotiation power and also a breach of sub-indent (k) of Annex I of the UTD because the consumer is not provided with any information of the consequences of variation and variation may be carried out without any valid reasons.

3.3.1.1.5 Clear-cut case of abuse – Assignment clause

Sub-indent (p) of Annex I of the UTD foresees that a standard term is possibly unfair if it gives the service provider the possibility of transferring his rights and obligations under the contract without the consumer’s agreement and the transference may serve to reduce the guarantees for the consumer.

Dropbox’s assignment clause contract is provided under “Miscellaneous legal terms” of the ToS. It states that a user “…may not assign any of [his] rights in these Terms, and any such attempt is void, but Dropbox may assign its rights to any of its affiliates or subsidiaries, or to any successor in interest of any business associated with the Services…” This is an example of an extremely one-sided assignment term. Clearly, Dropbox can assign all or any of his rights without the consumer’s agreement and consumer is not allowed to assign any of his rights under any circumstances. Such a clause is arguably unfair under sub-indent (p) of Annex I of the UTD.

3.3.1.2 UKFast

Being the only cloud service provider from Europe. Based in the UK, the company also promotes itself as being “UK's Best Dedicated Server Web Hosting”.118 It is also visible, that UKFast is mainly directed to businesses, not individual consumers. Nevertheless, “Customer” is defined as “…any person or organisation…”119 which implicates that also consumers can contract with UKFast. Although UKFast employs less severe contract terms than Dropbox, UKFast also has clauses which do not satisfy the criteria of effectiveness.

3.3.1.2.1 Time frame to initiate proceedings

UKFast is the only provider under analysis which limits the time frame to initiate proceedings against it. Clause 9.4 of the agreement provides that “…no action or proceedings against the Company arising out of or in connection with the

118 See <http://www.ukfast.co.uk/>, accessed 10 March 2014
119 Clause 1.12 of the T&Cs of UKFast.
Agreement shall be commenced by the Customer more than one year after the Services have been rendered…” This clause should be viewed as a barrier to seek a remedy because it reduces the prescription period and is to the detriment of the consumer. Imposing a limitation period against a consumer that is shorter than the limitation period prescribed in law is potentially unfair under sub-indent (q) of Annex I of the UTD which stipulates that a term is arguably unfair if it excludes or hinders consumers’ right to take legal action or exercise any other remedy.

3.3.1.2.2 Costs – Jurisdiction clause
Clause 25 of the ToS provides that the contract is “… governed by the laws of England and Wales and is subject to the exclusive jurisdiction of the Courts of England and Wales.” Although the jurisdiction is not conferred across the Atlantic Ocean, the consumer protection laws interfere in cases where the customer is not in England. For businesses, this term is arguably costly, because compared to consumers, it is more difficult to bring the proceedings to the home state of an enterprise. Thus, such a jurisdiction clause may make it difficult for an enterprise to enter an appearance.

3.3.1.2.3 Clear-cut case of infringement – Assignment
Similar to the assignment clause of Dropbox, the same clause in the T&Cs of UKFast is very one-sided. Thus, it implicates the abuse of superior negotiation powers. It prescribes that the “Customer shall not assign or transfer any of the Customer's rights or obligations under the Agreement without the prior written consent of the Company.” The clause links assignment with the consent provided by the provider while the provider can assign his rights at his sole discretion, without the agreement of the consumer, which is contrary to the rule set by sub-indent (p) of Annex I of the UTD.

3.3.1.2.4 Clear-cut case of infringement – Monitoring
The “Data Protection Support” of the T&Cs of UKFast provide that “Monitoring or recording of your calls, emails, text messages and other communications may take place in accordance with UK law, and in particular for business purposes, such as for quality control and training, to prevent unauthorised use of UKFast’s websites,

120 Clause 21 of the T&Cs of UKFast.
121 See 3.3.1.1.5 above.
to ensure effective systems operation and in order to prevent or detect crime.”
Clearly, monitoring in accordance with the law may be seen as a valid ground for
interception (provided that the principle of proportionality is observed). What
makes this term unfair in the eyes of the author, is that it allows monitoring, in
particular, for business purposes, without any safeguards to the customer. “Business
purposes” involve quality control and training, prevention of unauthorised use of
UKFast’s website, ensuring effective systems operations and prevention of crimes.
Thus, a customer may be monitored constantly.

3.3.2 Platform as a Service providers – Google Apps for Business and Windows Azure
PaaS is seemingly a concern of an enterprise, not a single consumer anymore. Thus,
the rationale discussed above and held by the author that SMEs should not be
devoid from protection against unfair terms becomes relevant.

3.3.2.1 Google Apps for Business
Google Apps is a service that provides independently customizable versions of
several Google products using a domain name provided by the customer. It features
several Web applications with similar functionality to traditional office suites,
including Gmail, Google Calendar, Docs, Drive, Groups, News, Play, Sites, Talk,
and Wallet.122

3.3.2.1.1 Transparency – Hidden terms
Hidden terms could be considered as terms that are accessible in a difficult manner.
Evidently, it is a matter of transparency.

According to the Additional Terms for Use of Additional Services Agreement
section 1123, the “additional services” are not provided under the Google Apps
Agreement, but provided to Customers via “default settings” (clause 3). This means
that when accepting the Google Apps Agreement, a customer is accepting to a
rather extensive list of additional services124 (54 services as of 28 March 2014, some
require written agreement ) which are offered to Customers on an opt-out basis. The

123 Additional Terms for Use of Additional Services Agreement, see
124 List of Google’s additional services <https://support.google.com/a/answer/181865?hl=en> accessed 11 April
2014.
questions here is, does the Google Apps Agreement give necessary indication of these 54 extra services or should these services to be thought as “secret”?

Clause 1 of the Additional Terms for Use of Additional Services Agreement provides a hyperlink to these additional services, but does not indicate the essence of them and there is a rather great possibility that this hyperlink is left unclicked by the customer.

Under clause 17 of the Additional Terms for Use of Additional Services Agreement, it is provided that “Google may modify these Additional Terms from time to time.” This does not indicate whether Google will notify the customer of any changes or what are the valid grounds to change the terms. Deciding under the UTD, this term is against sub-indent (j) of Annex I – enabling the seller to alter the terms unilaterally without a valid reason which is specified in the contract.

A justified fear arises when reading Google’s T&Cs that somewhere exist some extra (secret?) terms which are necessary for making an informed decision to contract with Google. This fact is contrary to the principle of transparency.

The French Data Protection Authority (CNIL) investigated Google’s Privacy Policy in 2012 and sent an extensive questionnaire to Google to give answers about the validity of the Privacy Policy under EU data protection law. One of the questions was explicitly related to Google Apps. In their answer, Google provides that the customer of Google Apps may “optionally enable additional Google services that are not part of the core Google Apps offering.” This refers to an opt-in model, not to an opt-out regime, which is contrary to the clause 3 of the Additional Terms for Use of Additional Services which states that “If You are a new Customer who has signed up on or after November 9, 2010, the Additional Services are provided on an "opt-out" basis. The default setting for the Additional Services is on.”

125 Question 47, directed to Google: “Concerning Google Apps, which is offered in several versions, including a “free” version, a “business” version and an “education” version:
A) Please indicate any specific rules that apply to the combination of data for Google Apps end users who are employed by companies, public agencies and education establishments.
B) Please provide specific distinctions that may apply to different versions of Google Apps, if any exist.” The questionnaire is accessible via the website of CNIL at <http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-cnil-sends-a-detailed-questionnaire-to-google/> accessed 22 June 2014.

3.3.2.1.2 Costs – Jurisdiction clause
Clause 14.10 of the Google Apps for Business Online Agreement stipulates that “This Agreement is governed by California law, excluding that state's choice of law rules. For any dispute arising out of or relating to this agreement, the parties consent to personal jurisdiction in, and the exclusive venue of, the courts in Santa Clara County, California.” As the jurisdiction clause confers jurisdiction in the U.S, see 3.3.1.1.2 above.

3.3.2.1.3 Time/Abuse of negotiation powers – Overlong curing period for the provider in case of termination
Although not a clear-cut situation of abuse of negotiation powers, the author sees issues with Google’s termination clause. Clause 11.1 of the Google Apps for Business Online Agreement provides that both parties “may suspend performance or terminate the agreement on similar grounds: (i) the other party is in material breach of the Agreement and fails to cure that breach within thirty days after receipt of written notice; (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) the other party is in material breach of this Agreement more than two times notwithstanding any cure of such breaches.”

Unfortunately the T&Cs of Google do not provide a definition of a “material breach”, thus it is a matter of interpretation and consequently creates ambiguity. Similarly, the termination clause of SaaS providers Salesforce.com and Dell Boomi link the right to terminate with the notion of “material breach” while not defining what constitutes a material breach. Clause 12.3 of the Master Subscription Agreement of Salesforce.com provides that both parties may terminate the contract prior to a 30 days notification if there is a “material breach” and this remains uncured. Commercial Terms of Sale of Dell Boomi provide that either party may terminate this Agreement by notice in writing immediately if the other party commits a material breach and fails to remedy such a breach within 30 days of written notice (clause 14.1).
and seeks to lock in the service user even after the harm has been caused. Thus, it can be considered unfair under the sub-indent (q) of Annex I of the UTD\textsuperscript{128} because it prescribes an unreasonably long curing period and subsequently the customer’s right to seek an effective remedy is hindered.

3.3.2.2 Windows Azure

Windows Azure is an open and flexible cloud platform that enables its customers to quickly build, deploy and manage applications across a global network of Microsoft-managed data centres. The customer can build applications using any language, tool or framework.\textsuperscript{129}

3.3.2.2.1 Costs – Termination

The termination clause of Windows Azure’s T&C provides that “You may terminate this Subscription at any time during its Term; however, you must pay all amounts due and owing before the termination is effective, and no refunds will be provided.”\textsuperscript{130} As discussed in 3.3.1.1.1 above, such a termination clause must be seen as a barrier to seek a remedy – to terminate the contract. If no refunds are provided, the customer has to be very specific on the dates when to terminate and, therefore, terminating “at any time” might prove to be disadvantageous to the customer.

3.3.2.2.2 Costs – Jurisdiction

If the customer chooses the location of “Europe”, the T&Cs of Windows Azure confer jurisdiction to the courts of the Republic of Ireland.\textsuperscript{131} Not to be repetitive, see 3.3.1.2.2 above.

3.3.2.2.3 Clear-cut case of abuse of negotiation power – Assignment

Under “Miscellaneous” section 9(b), the laconic assignment term of Windows Azure is provided: “You may not assign this agreement either in whole or in part.”

\textsuperscript{128} Indent (q) of Annex I of the UTD provides that a standard term may be regarded as unfair if it excludes or hinders “the consumer’s right to take legal action or exercise any other legal remedy, particularly requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions, unduly restricting the evidence available to him or imposing on him a burden of proof which, according to the applicable law, should lie with another party to the contract.”


\textsuperscript{130} Clause 4(b) of the ToS of Windows Azure.

\textsuperscript{131} Clause 9(h) of the T&Cs of Windows Azure provide that the agreement is “...governed by the laws of Ireland. If we bring an action to enforce this agreement, we will bring it in the jurisdiction where you have your headquarters. If you bring an action to enforce this agreement, you will bring it in Ireland...”
This term is imbalanced, because it explicitly provides that Windows could assign the agreement, while the Customer’s right to do the same is excluded. Such an assignment clause is possibly unfair under sub-indent (p) of Annex I of the UTD.

3.3.3 Software as a Service platform providers – Salesforce.com and Dell Boomi

3.3.3.1 Salesforce.com

Salesforce.com is a global cloud computing provider from the U.S and is best known for its CRM system. Salesforce.com is an example of a SaaS provider. It has more than 2,100,100 subscribers worldwide.\(^{132}\)

3.3.3.1.1 Transparency/Inequality of bargaining power – Termination

Termination clause is provided in the Salesforce.com’s Master Subscription Agreement (MSA). Clause 12.3 of the MSA provides that “a party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy ....”

Seemingly, the clause is balanced, because it does not differentiate between the provider and the customer. Both are given a ground for termination if a material breach is uncured during 30 days of the event. As the MSA does not specify what constitutes a “material breach”, it is up for interpretation and therefore does not provide sufficient transparency for the customer. This may constitute an infringement under article 5 of UTD because the terms must be in “plain and intelligible language”. It is clearly an indication of the inequality of bargaining power because under this clause, the termination is greatly dependent on the discretion of the provider. This clause goes against the “plainness” rule, because it is not providing a clear picture to the customer when the termination is possible (foreseeable consequences).

Also, the termination clause of Salesforce.com foresees an overlong curing period, which is arguably unfair under sub-indent (q) of Annex I of the UTD as it hinders the customer’s right to seek a remedy.

3.3.3.1.2 Costs – Jurisdiction
Clause 13.1 of the MSA of Salesforce.com confers jurisdiction to the courts of England and the law governing the contract is also the one of England’s. For analysis, see 3.3.1.2.2 above. Taking into account that Salesforce.com is directed to businesses, it is likely that a company domiciled in, e.g. the Netherlands should have to go courts in England.

3.3.3.1.3 Inequality of bargaining power – “Whole agreement clause”
Clause 14.3 of the MSA provides that the MSA is “the entire agreement between you and us regarding your use of Services and Content.” L. Trakman provides that “whole agreement” clauses are the extreme form of click-wrap agreements because such clauses implicitly seek to impede a finding that “a condition is ambiguous, or that it should be interpreted in light of standards of reasonableness that are extraneous to the contract.”¹³³ Entire agreement clauses ensure that parties cannot be tied with obligations or found liable for representations that are not included in the T&Cs. Thus, it is a sign of abuse of negotiation powers because the drafting of the contract is totally in the hands of the provider and interpretation of the contract is strictly limited with the plain meaning of the contract.¹³⁴

3.3.3.2 Dell Boomi
Dell is a CIF certified cloud service provider and therefore chosen for analysis for this thesis. CIF, as said above, is a soft law initiative to enhance transparency in the T&Cs of a cloud service provider. As with Salesforce.com, Dell Boomi is not aimed at consumers (B2C), but mainly for B2B customers.¹³⁵ Dell Boomi’s T&Cs find the least amount of reproaches by the analysis.

3.3.3.2.1 Time/Abuse of bargaining power – Termination clause
Similarly with the termination clause of Salesforce.com’s, clause 14.1 of the T&Cs provide that “Either party may (without prejudice to any other rights or remedies it may have against the other party) terminate this Agreement by notice in writing immediately if the other party: 14.1.1 commits a material breach of the Agreement and fails to remedy such breach within 30 days of written notice....” Thus, it can

¹³⁴ See supra note 40 above.
similarly be concluded that the termination clause of Dell Boomi’s abuses the superior bargaining position when it employs an overlong curing period (see 3.3.2.1.3 above).

3.3.3.2 Costs – Jurisdiction clause

Clause 19.7 provides that “The Agreement and any non-contractual obligations shall be interpreted according to English law and the English courts shall have exclusive jurisdiction.”

Not to repeat what has already been discussed, see 3.3.1.2.2 above and 3.3.3.1.2 above 3.3.1.1.2 above.

3.4 Consumer Protection Regime in Estonian Law

Sections 3.4 and 3.5 turn to Estonia’s and United Kingdom’s consumer protection regimes. As this thesis aims to broaden the scope of protection against the unfair terms also to SMEs, the comparative approach is necessary to indicate the differences of these two EU Member States.

Regulation of B2C contracts is incorporated in the Law of Obligations Act (LOA)\textsuperscript{136} of Estonia which entered into force on the 1 of July 2002. Estonian legal system belongs to the civil law system and is mainly influenced by the German law and it’s Civil Code (\textit{BGB}).\textsuperscript{137}

General terms about standard contract are regulated in §§ 32-45 of the LOA. Section 39 provides the rule for interpreting the standard terms. Section 39(1) states that “standard terms shall be interpreted according to the meaning that reasonable persons of the same kind as the other party would give to them in the same circumstances. In the case of doubt, standard terms shall be interpreted to the detriment of the party supplying the standard terms.”\textsuperscript{138} Therefore, the threshold for interpreting the standard terms is what a similar reasonable person would give to the situation under the same circumstances. The term also implies that a standard term is always interpreted to the detriment of the service provider. Under § 39(2), a void

\textsuperscript{136} Law of Obligations Act, RT I 2001, 81, 487.
\textsuperscript{138} LOA § 39(1).
standard term cannot be interpreted in such a way to give its content a meaning under which it would be valid.

Section 42(1)\textsuperscript{139} stipulates that “a standard term is void if, taking into account the nature, contents and manner of entry into the contract, the interests of the parties and other material circumstances, the term causes unfair harm to the other party, particularly if it causes a significant imbalance in the parties' rights and obligations arising from the contract to the detriment of the other party. Unfair harm is presumed if a standard term derogates from a fundamental principle of law or restricts the rights and obligations arising for the other party from the nature of the contract such that it becomes questionable as to whether the purpose of the contract can be achieved. Invalidity of standard terms and the circumstances relating thereto shall be assessed as at the date of entry into the contract.” This is the general rule of unfairness. As with article 3(1) of the UTD, the requirement of “significant imbalance” is similar in Estonian law. But, § 42(1) includes an extra rule of presumption of unfairness when a fundamental principle of law is breached. Meaning that if a principle of legal certainty and clarity (transparency) is breached, a standard term in a standard contract is unfair therefore void.

Section 42(3) is the equivalent of Annex I of the UTD. It is different from two aspects. Firstly, it is more extensive than the minimum harmonisation directive, stating 37 grounds under which a standard term is considered to be unfair.\textsuperscript{140} Secondly, these grounds stipulated in paragraph 3 constitute a black list (not a grey list like Annex I of the UTD) of standard terms which are void by law, without the party having to prove the unfairness.\textsuperscript{141}

Analysing standard terms through the prism of § 42(3) is the first step in the unfairness enquiry under Estonian law because they provide an automatic knock-out mean – list of void terms. If the disputable standard term cannot be scrutinised under the black list, the analysis turns as a second step to the general rule under § 42(1) under which the claimant must prove that a standard term is contrary to the principle of good faith, but not unfair. Also, under the second sentence of the

\textsuperscript{139} Transposition of article 3(1) of the UTD into Estonian law.
\textsuperscript{140} Section 42 paragraph 3 states that this extensive list of unfair terms is not a closed list (\textit{numerous clausus}).
paragraph 1, the claimant must not prove unfairness, but that the term infringes a principle of law.\textsuperscript{142}

Under § 44 of the LOA, if a standard term is used in a B2B contract, the list of unfair terms provided under § 42(3) are presumably unfair, making it a grey list for the B2B contracts.\textsuperscript{143} Hence, § 42(3) expands also to B2B contracts.\textsuperscript{144} Businesses receive a lesser degree of protection under the standard terms regulation than consumers, but the rationale that a standard term can be unfair for a B2B contract is enshrined in Estonian law. The seller has an opportunity to prove that using a disputable term is a common practice in the industry and therefore not unfair.\textsuperscript{145} Nevertheless, the law provides a presumption against the user of the standard terms which is conceivably a heavy burden of proof in the court proceedings.

\textbf{3.4.1 Unfair terms of six service providers through the prism of Estonian consumer law}

Looking at the black list of prohibited standard terms under § 42(3) closely, several similarities with the Annex I of the UTD are noticeable, but it also includes some more stringent rules. The analysis under Estonian law is hypothetical. None of the service providers confer jurisdiction to Estonian courts by their T&Cs.

Section 42(3)(9) stipulates that a standard term is unfair if it “prescribes an unreasonably short term for the other party to submit claims, including an unreasonably short limitation period for claims arising from the contract or law.” This would mean that under Estonian law, clause 9.4 of UKFast’s T&Cs (see 3.3.1.2.1 above) – stating that the customer may only bring proceedings against the provider during one year period after which the services have been rendered – would be considered unfair in a B2C contract and would be presumably unfair in a B2B contract because § 146(1) of the General Part of the Civil Code Act\textsuperscript{146} provides that the general limitation period arising from a contract is three years.

\textsuperscript{142} Ibid, p 149.
\textsuperscript{143} Section 44 of the LOA: “If a standard term specified in subsection 42 (3) of this Act is used in a contract where the other party to the contract is a person who entered into the contract for the purposes of the economic or professional activities of the person, the term is presumed to be unfair.”
\textsuperscript{144} Confirmed by the Supreme Court of Estonia in a Judgement of 13 September 2004, Case No 3-2-1-88-04. Available at <http://www.riigikohus.ee/?id=11&indeks=0,2,10246,10624,10627&tekst=RK/3-2-1-88-04> para 13.
\textsuperscript{145} P. Varul, I. Kull et al. “Võlaõigusseadus I Kommenteeritud vlj”, p 166.
\textsuperscript{146} General Part of the Civil Code Act, RT I 2002, 35, 216.
Section 42(3)(10) foresees that a standard term is void (and presumably unfair for businesses according to § 44 of the LOA) if it “deprives the other party of the opportunity to protect the party's rights in court or unreasonably hinders such opportunity from being exercised.” This term is the Estonian equivalent of sub-indent (q) of Annex I of the UTD.\textsuperscript{147} Therefore, the jurisdiction clauses of UKFast, Google Apps for Business, Windows Azure and Salesforce.com are unfair and thus void in a B2C standard form contract and presumably unfair in a B2B contract under Estonian law with the burden of proof lying on the suppliers’ to prove that the term is not unfair.

Section 42(3)(14)\textsuperscript{148} foresees the similar variation term provided in the Annex I sub-indent (j) of the UTD and therefore standard terms about variation without a valid ground specified under the contract are also unfair under Estonian law (e.g. see Dropbox’s variation clause in 3.3.1.1.43.3.1.1.4 above).

Similarly as Annex I sub-indent (p) provides the rule about the prohibition of assigning rights under the contract if this reduces the guarantees under the contract, § 42(3) (25)\textsuperscript{149} provides the same rule. Thus, Dropbox’s (see 3.3.1.1.13.3.1.1.5 above), UKFast’s (see 3.3.1.2.3 above) and Windows Azure’s (see 3.3.2.2.3 above) assignment clauses are void under Estonian law on the grounds of § 42(3)(25).

Although it must be noted that the condition for considering an assignment clause unfair are different under Estonian law and the UTD. Under § 42(3)(25), the term is unfair if the rights are assigned without the consent of the other party on the condition that it reduces “likelihood of the contract being performed” whereas under sub-indent (p) of Annex I of the UTD, the rule prescribes that the transferring of rights cannot reduce the guarantees of the consumer under the contract. Also, sub-indent (p) does not set a requirement of consent from the other party for the transfer of rights.

\begin{itemize}
\item \textsuperscript{147} See \textit{supra} note 128.
\item \textsuperscript{148} A standard term is unfair, in particular, if it “prescribes the right of the person supplying the term to alter the terms or conditions of the contract unilaterally for a reason or in a manner not provided by law or specified in the contract.”
\item \textsuperscript{149} A standard term is unfair under indent 25 if it “provides the party supplying the term with the right to transfer the rights and obligations thereof arising from the contract to a third party without the consent of the other party where this may serve to reduce the likelihood of the contract being performed.”
\end{itemize}
Section 42(3)(29) provides a similar ground of unfairness as the UTD Annex I sub-indent (f) which delivers that a term is unfair if it “provides the party supplying the term with the right to terminate the contract without giving reasons for the termination if the same right is not provided to the other party.” It must be noted that none of the T&Cs analysed stipulated a term of such gravity.

Section 42(3)(33) prescribes that a standard term is unfair if it “provides… the right to terminate a contract … for an unspecified term without good reason and without a reasonable period of advance notice.” If the term of contract is left unstipulated, the seller must provide a notice within a reasonable period with a valid reason. This questions the fairness of clauses which prescribe that the seller is allowed to stop (in essence has similar effect as termination to the customer) providing services on a discretionary basis.\textsuperscript{150}

\textsuperscript{150} For example, see Dropbox’s ToS which stipulate that they can “…stop, suspend, or modify the Services at any time without prior notice to you. We may also remove any content from our Services at our discretion.”
3.5 Consumer Protection and UK law

Under this section, the author focuses on three pieces of statutory law of the UK – the Unfair Contract Terms Act (UCTA) 1977, Supply of Goods and Services Act (SGSA) 1982 and the Unfair Terms in Consumer Contracts Regulations (UTCCR) 1999. Contrary to Estonian law, the UK law provides main principles regarding the unfairness of a standard term, not an extensive black list. The regulation of unfair terms relies on the principles described below, but also to the UTCCR which transposes the UTD into UK law. Furmston highlights that the UK Parliament has so far decided for a piecemeal approach to consumer protection legislation, because it has operated by the prohibition or regulation of exemption clauses in particular types of contracts instead of enacting rules applicable to all consumer contracts.151

3.5.1 Unfair Contract Terms Act (UCTA), 1977

Furmston notes that the title of UCTA is grossly misleading, due to the fact that it does not deal with all unfair contract terms, but only with unfair exemption clauses.152

Sections 2-7 are the core of the UCTA.153 Section 3(1) stipulates rules about “dealing as a consumer.”154 The section provides that “contracting parties where one of them deals as a consumer or on the other’s written standard terms of business”, the seller cannot stipulate in the contract that his liability is excluded or restricted in respect of the breach155 or is authorised to perform substantially different from that which was reasonably expected of him or not render no performance at all, except in so far as the contract term satisfies the requirement of reasonableness.156

Section 4(1) prescribes that a person dealing as a consumer cannot by reference to any contract term be made to indemnify another person in respect of liability that may be incurred by the other for negligence or breach of contract, except in so far as the contract term satisfies the requirement of reasonableness.

---

152 Ibid, p 232.
154 See also section 12 of the UCTA.
155 UCTA section 3(2) (a).
156 UCTA sections 3(2) (b) (i-ii).
As visible, the requirement of reasonableness is an important factor of UCTA and works as a filter of determining whether a term is unfair or not.

Section 11 of the UCTA states that the requirement of reasonableness “is that the term shall have been a fair and reasonable one to be included having regard to the circumstances which were, or ought reasonably to have been, known to or in the contemplation of the parties when the contract was made.”\(^{157}\) The requirement of reasonableness cannot be seen separately from the Schedule 2 of UCTA, which provides considerations for the application of the test, e.g. the strength of the bargaining positions of the parties relative to each other\(^ {158}\), was the customer induced to agree to the terms, or did he have alternative opportunities of entering into a similar contract with other persons\(^ {159}\), did the customer knew or ought reasonably to have known about the existence and extent of the term.\(^ {160}\) The burden of proof regarding reasonableness lies with the one who claims the term is reasonable.

### 3.5.2 Sale of Goods and Services Act (SGSA), 1982

Part II of the SGSA deals with contracts for the supply of services. Under section 12, a contract for the supply of a service is a contract where the supplier agrees to carry out a service, irrespective of whether the or not the goods are transferred or to be transferred or bailed or to be bailed by way of hire and regardless of the nature of the consideration for which the service is to be carried out.\(^ {161}\)

Section 13 of the SGSA stipulates the grounding rule of service contract – “in a contract for the supply of a service where the supplier is acting in the course of a business, there is an implied term that the supplier will carry out the service with reasonable care and skill.”

As Reed and Cunningham point out, the common law basis of the reasonable care and skill comes from a 1957 case of *Bolam v Friern Hospital Management Committee*\(^ {162}\) which stated that the test for reasonable care and skill in medical standards are not to be assessed by “the ordinary man”, but the “ordinary skilled

\(^{157}\) Section 11(1) of the UCTA.

\(^{158}\) Schedule 2(a) of the UCTA.

\(^{159}\) Schedule 2(b).

\(^{160}\) Schedule 2(c).

\(^{161}\) Section 12(1), (3) of the SGSA.

\(^{162}\) *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582.
man exercising and professing to have that special skill.” Therefore, analysing whether the cloud service provider has performed his duties with reasonable care and skill, one has to determine the skill of an “ordinary skilled company” exercising that particular art.

Reasonableness is the leading notion also in sections 14 and 15 of the SGSA, providing that if not agreed in the contract, the service must be performed within a reasonable time and if the consideration is not agreed, the customer must pay a reasonable charge in exchange of the service.

### 3.5.3 The Unfair Terms in Consumer Contracts Regulations (UTCCR), 1999

As mentioned above, the UTCCR is transposing the Unfair Terms Directive of 1993 into UK law. It came into force on July 1, 1995. Thus, the definition of an “unfair term” in article 3(1) of the UTD and section 5(1) of the UTCCR are identical. Section 8(1) stipulates that an unfair term is not binding to the consumer (article 6(1) of the UTD). Also, the Annex I has been transposed into the UK law as unchanged. Thus, not to be repetitive, see sub-section 3.2.1 above about the Unfair Terms Directive of EU.

### 3.5.4 Unfair standard terms under the UCTA, SGSA and UTCCR

Section 27(2) of the UCTA states that the Act has effect notwithstanding any contract term that applies or purports to apply the law of some country outside the UK where (either or both) the term appears to the court, or arbitrator or arbiter to have been imposed wholly or mainly for the purposes of enabling the party imposing it to evade the operation of this Act; or in the making of the contract one of the parties dealt as consumer, and he was then habitually resident in the UK and the essential steps necessary for the making of the contract were taken there, whether by him or by others in his behalf. Consequently, if a consumer is

---

164 Ibid, p 22.  
165 Section 14 of the SGSA.  
166 Section 15(1) of the SGSA.  
168 Section 27(2) of the UCTA.
habitually resident in the UK, the UCTA will not allow a cloud service provider to impose any other law than the UK’s.\textsuperscript{169}

According to Reed and Cunningham, clauses which provide a relatively short period to initiate proceedings under the standard terms (e.g. UKFast, see 3.3.1.2.1 above), the English courts would invoke sub-indent of (q) Schedule 2 of the UTCCR, because it “hinders a consumer to take legal action” against the provider.\textsuperscript{170} Arguably, in the context of jurisdiction, the location of the competent court may also affect the remedial situation and therefore sub-indent (q) of the UTCCR (and UTD) arguably expands to these situations.

Variation of contract terms without a valid ground is therefore similarly unfair under sub-indent (j) of the UTCCR as under sub-indent (j) of the UTD. Thus, the variation clause of Dropbox is arguably unfair under UK law.


\textsuperscript{170} Identical clause to the sub-indent (q) of Annex I of the UTD.
3.6 Findings and Opinion

Section 3.3 analysed the T&Cs of six cloud providers deploying all three cloud offering models. The analysis sought to answer the research question – whether the remedial situation between the customer and the cloud service provider could be considered as an “effective” one? To reach measurable conclusions, information about the remedial situation was obtained analysing the standard term contracts from the prism of criteria of effectiveness – four main barriers to seek a remedy. These barriers include transparency; time; cost and definite cases of inequality of bargaining power which all influence the remedial situation.

Standard terms by their essence, do not provide equality, because the terms are drafted in advance by the service provider and the customer cannot influence their content. Nevertheless, the improvement in the remedial situation might raise trust towards the cloud, thus, leading to a greater number of subscriptions. The analysis shows that cloud providers clearly take advantage of their superior bargaining power to impose one-sided terms upon the customer. Thus, the rationale imposed by Oceano that consumers need protection vis-á-vis the sellers because they abuse their negotiation powers is valid. Contract law does not provide sufficient protection to the weaker parties of the contract. Protection against unfair terms is a vital shield to the consumers, who would otherwise be thoroughly exploited. As discussed, also smaller businesses require protection from abuse of bargaining power, suffering from the same take-it-or-leave-it contracting situation.

IaaS service providers Dropbox and UKFast deliver storage to their customers. By the essence of their business model, they hypothetically contract with the largest amount of consumers, while PaaS and SaaS are more directed towards businesses who deliver their own services to consumers and/or businesses. Sadly, Dropbox places the severest barriers to seek an effective remedy. Dropbox’s T&Cs lack transparency when the company deploys a termination clause which is divided by two separate policies (Acceptable Use Policy and Pricing Terms and Conditions) and only after reading the two policies, the clear remedial picture is provided to the customer. AUP provides that the customer is free to terminate the contract at any given moment, while the PTC highlights that no refunds are provided if the payment for the service has been made in advance.
Similarly, conferring jurisdiction in the United States, Dropbox forces the customers to make extra costs for seeking a remedy which acts as a definite barrier. Also, if a European customer would need to cross the Atlantic to resolve a service contract dispute in the U.S, it would make him harder to enter appearance and such a jurisdiction clause would discourage litigation against the cloud service provider. Thus, jurisdiction clauses have a twofold barrier effect – costs and making an appearance in court. From the perspective of consumer law, it is fair to conclude that any jurisdiction clause conferring jurisdiction away from the domicile of the consumer would be considered unfair under sub-indent (q) of Annex I of the UTD.171

Dropbox’s T&Cs also display clear-cut cases of abuse of bargaining power when the terms provide that instead of the service provider, the customer is the one responsible for maintaining and protecting all of the information uploaded to the cloud. Clearly, Dropbox seeks that customers would encrypt their data prior to uploading it to the cloud, but in the opinion of the author, if this is not done by the customer (and in most cases it is not), the service provider should foresee that unencrypted materials would also be protected and responsibility for such protection is not excluded. After uploading the files, the customer cannot access the servers and control the storage of such files. Customer’s control is limited to access to the website of Dropbox via its web browser.

Also, as examples of inequality of bargaining power, assignment, modification and variation clauses of Dropbox are analysed and found imbalanced and unfair under sub-indices (p), (j) and (k) of Annex I of the UTD.

UKFast’s T&Cs provide less severe remedial situation to its customers compared to Dropbox, however, still failing to provide an effective remedial situation.

UKFast is the online provider which limits the time frame under which the customer may initiate proceedings against the service provider. As the “time” factor is one of the criteria of effectiveness, UKFast fails to deliver an effective remedial situation. For example, the usual prescription period from a contract is three years – UKFast shortens it to one year. Thus, in a hypothetical contracting situation between an

171 This holds for all jurisdiction clauses, not only for those which confer jurisdiction to the courts of the U.S. See supra note 110 about the CJEU case Oceano.
Estonian customer and UKFast, the prescription period would be shortened three times compared to law, since, imposing a barrier to seek a remedy.

UKFast also employs standard terms which constitute clear-cut cases of infringement, e.g. the assignment clause of UKFast can be considered unfair under sub-indent (p) of Annex I of the UTD. Also, UKFast provides a monitoring clause in its Data Protection Support which allows constant monitoring of customer’s activities for questionable motives.

PaaS service providers Google Apps for Business and Windows Azure also receive condemnation from the author. Google Apps for Business’s T&Cs lack sufficient transparency and, consequently, cannot be considered to deliver an effective remedial situation. The main reprimand to Google’s T&Cs is made because of the use of Additional Services, which a user are bound by if it agrees the T&Cs of Google Apps for Business. These Additional Services include an extensive list of services offered by Google on an “opt-out” basis. The T&Cs of Google Apps for Business Online Agreement provide insufficient indication to these Additional Services and, thus, the customer is bound by another set of (hidden) standard terms.

Also, the termination clauses of Google Apps for Business and Dell Boomi are considered imbalanced because they provide the cloud service providers with an extremely long curing period which has to lapse before the customer is allowed to terminate the contract.

Windows Azure’s T&Cs cannot be considered to provide an effective remedial situation because it provides barriers related to costs. Firstly, it introduces a termination clause (similar to the one of Dropbox) which does not allow the customer to receive refunds in case of termination. The T&Cs provide the customer with a freedom to terminate at any time, while if no refunds are provided, on the contrary, the customer has to be very precise on the dates when to terminate and, thus, the termination clause cannot no longer be considered effective. From the category of clear-cut infringements, Windows Azure deploys an unfair assignment clause.

SaaS service providers Salesforce.com and Dell Boomi receive the least amount criticism under this analysis. From the criteria of effectiveness, Salesforce.com
faces problems with inequality of bargaining power – imposing a vague termination clause in combination with the “entire agreement” clause which is to the detriment to the consumer and violates the principle of transparency.

The author considers the T&Cs of Dell Boomi to be the least severe and the remedial situation can be considered acceptable, while only minor reprimands made by the author.

The comparative analysis of the consumer protection laws of Estonia and UK law is aimed to provide proof of the different approaches taken by the EU Member States. Estonian law has made the Annex I of the UTD as a blacklist of unfair terms, simplifying the situation to the consumers, while in the UK, with the UTCCR, the UK has opted to enforce the Annex I of the UTD as a grey list of unfair terms, leaving more discretion to the court. Under Estonian law, also SMEs receive protection against unfair terms while in the UK, standard terms in B2B contracts can be considered unfair only if the stronger party to the contract employs extremely harsh exemption clauses. Thus, rendering the situation much more complicated to the SMEs. As the thesis argues that SMEs should also be protected from unfair terms, the author empathises the policy option of Estonia.

In total, the remedial situation of the six cloud providers cannot be considered as an effective one due to the fact that all of the service providers (representing all three service models) set barriers to seek a remedy, thus, not adhering to the criteria of effectiveness.

The remedial situation must be improved to build trust.\footnote{Clearly, trust is a complicated term to define. As Brooks explains, it contains both rational cognitive and emotional affective aspects. See F. B. Cross, “Law and Trust.” Georgetown Law, Forthcoming; McCombs Working Paper No. IROM-05-05; U of Texas Law, Law and Econ Research Paper No. 064. Available at SSRN: <http://ssrn.com/abstract=813028>, p 5-19. Trust is seen by the author as a value exchange, making an exchange with a service provider when the customer does not have full knowledge about the provider and his intent. It also involves hope that the vulnerabilities of the customer are not viciously used by the service provider. Trust towards such service providers could also be a mistake and the outcome of this analysis hints that some of the trust put upon the providers is clearly not deserved.}

Trust is the essential ingredient of a contractual relation, more so online, and at its current state, the customers and consumers are rightfully cautious of uploading their more sensitive data to the cloud. There must be a shift in the cloud market to raise confidence toward their services; however, this cannot be done artificially. For example, one
way to raise trust towards the customers is by being signatories to different assurance seals which could raise their trustworthiness in the eyes of the customers. The better the public reputation, the more public trust a service provider receives. The next chapter of the thesis focuses on assurance seals and aims to find out whether these certifications improve or have the potential to improve the remedial situation between the service providers and customers while at the same time raising trustworthiness.
4. Soft law and Assurances

The thesis analyses the T&Cs of cloud providers and asks if the remedial situation provided by these providers can be considered as “effective” from a consumer’s perspective. Problem with the service providers is that they want to look trustworthy and are members of different certifications which promote themselves as providing transparency (lessen the barriers to seek a remedy) and via these soft-law initiatives attract more customers to their services. By joining and adhering to different certifications, the providers are saying “you can trust me” – they seek to provide the customer an assurance. This chapter analyses the soft-law initiatives and assurances provided by these tools and aims to conclude if different certifications improve the remedial situation – to which they are aimed for – in favour of the cloud customers.

Cloud service providers’ success is largely dependent on how trustworthy they appear to their clients. Though, trust is a difficult currency to make business with and the service providers should keep in mind the words said by an unknown author: “Trust is like paper. Once it is crumpled, it can never be perfect.” Trust is related to several factors, one of them being the remedial situation. Badger et al. correctly highlight that offering insufficient remedies to a customer of a cloud service is not a viable business case in the long-term.\(^{173}\) Soft law is a self-regulatory instrument which may influence the behaviour of the market and its actors in a specific field.\(^{174}\) This chapter focuses on certifications and/or assurances in the field of cloud computing because in private relations, it is a way for the market actors to show initiative and therefore withhold government regulation. Although, it must be recognised that soft law’s main disadvantage is its lack of enforcement. Gersen and Posner highlight that soft law’s indirect nature at first sight can be overturned if the acceptance of the rules provided by the instrument is followed by many. The greatest example of such an instrument is The Universal Declaration of Human Rights.\(^{175}\) Soft law’s influence could be seen under two theories. Firstly – under the signalling theory – the communication by the self-regulatory instrument provides


\(^{175}\) Ibid, p 3 and 17.
Thus, signals may reduce uncertainties of cloud service users by providing them with information about the characteristics of the service provider otherwise unobservable to the customer. According to the signalling theory, the signal must be costly to be effective and credible. In the context of cloud computing, this means that the signal (assurance) must be audited by an independent third party. Clearly, self-certifications’ credibility is lower, but the “cost” criteria of the signalling theory may be fulfilled when a provider devotes significant amount of time to be compliant to the rules of the self-certification seal. It is of no dispute that self-certification is less credible than an audit by an independent third party because it is less probable that any mishaps will be brought to light. Secondly, the trust theory of assurances prescribes that trust is built by cognitive process, by prediction, intentionality and transference. Prediction infers that a certification provides necessary information for a user to evaluate the provider’s intentions and predict the future behaviour of a service provider. Prediction is therefore linked with certainty. Transference on the other hand aims to link the cloud service provider and a trustworthy certification authority as one in the eyes of the consumer. It has been empirically shown by Nöteborg et al. that third party assurance seals lead to lower privacy and integrity concerns compared to providers who do not offer any assurances or offer vendor-provided assurances. Hence, assurances provide trust in the electronic commerce.

Assurances are meant to mitigate uncertainties arising from contracting with a cloud service provider and are meant to be facilitators of trust. Repeated multiple times, trust is the keyword in the Internet and reacts to suspicions arising from security, privacy and seller’s integrity. For example, Sunyaev and Schneider point out that users of cloud services do not necessarily know which cloud services (platforms can

177 Concerning security, privacy, transparency, availability, remedies, interoperability and legal compliance.
be stacked, e.g. in case of Dropbox) customers are using and where their data will be processed and located for storage. Such circumstances facilitate untrustworthiness.\(^{184}\)

Research conducted by Lansing et al. proves that privacy and security are the most important assurances. Their research focused on 10 assurances offered by seven cloud certifications. The assurances analysed were availability, contract\(^{185}\), customer support, financial stability, flexibility, interoperability, legal compliance, privacy, process maturity and security. The fact that privacy and security assurances were two top-ranked assurances is not surprising. Interestingly, “contract” was ranked fifth in the ten assurances; the last two were financial stability and flexibility. Concerning the seven cloud certifications analysed by Lansing et al., only EuroCloud\(^{186}\) focuses on all of the ten assurances. SaaS-EcoSystem, Trust in Cloud\(^{187}\) focus on nine of the assurances (excluding process maturity). Other certifications focus mainly on privacy (e.g. TRUSTe) or security (Cloud Security Alliance).\(^{188}\)

An important standard-setting soft law regulation in the field of electronic commerce is promulgated by the OECD – Guidelines for Consumer Protection in the Context of Electronic Commerce, from 1999.\(^{189}\) This initiative highlights that “the electronic marketplace requires a global approach to consumer protection as part of a transparent and predictable legal and self-regulatory framework for electronic commerce.”\(^{190}\) OECD Guidelines represent the necessary principles for a transparent and fair remedial situation. Part IV.B of the Guidelines about


In J. Lansing et al., “Cloud Service Certifications: Measuring Consumers’ Preferences for Assurances”, p 5. Contract as an assurance in their research means that the “provider offers understandable contractual arrangements that meet common business practice and the contract terms do not restrict the customer’s property rights of their data stored in the cloud service.”

\(^{185}\) See <http://www.eurocloud.org/> accessed 22 June 2014.


\(^{187}\) J. Lansing et al., “Cloud Service Certifications: Measuring Consumers’ Preferences for Assurances”, p 5, 8. Limitations of the research must be provided: research was conducted by the data collected from 53 respondents whose average age was 26, 9 years (81% of them were male, 19% female). 49 percent of the 53 respondents were university students and 53% of the 53 respondents used the cloud for private use only. 40 percent used the cloud for private and business use (mix-use) and only 2 percent had selected professional use only. Research method was Best-Worst Scaling (BWS).


\(^{189}\) OECD Guidelines – Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce. Part II of the Guidelines also promotes the necessity that businesses should not use unfair contract terms.
“Alternative Dispute Resolution and Redress” highlights that “consumers should be provided meaningful access to fair and timely alternative dispute resolution and redress without undue cost or burden.” To achieve this, the Guidelines provide that governments, businesses and consumers have to co-operate.

The following sections of this chapter focus on Cloud Industry Forum’s Code of Practice (promoting transparency), Cloud Security Alliance STAR (security and transparency) and TRUSTe (data privacy).

4.1 Cloud Industry Forum (CIF)

4.1.1 Introduction

Cloud Industry Forum commercialises itself under the devise that it is “Championing Transparency and Trust of Online Services.”191 It is brought as a good example of how companies should deal with consumers and what information should be provided to them by Reed and Cunningham.192 CIF Code of Practice (CoP)193 is a tool intended to improve transparency for the end-users.194 It is based on three pillars – Transparency, Capability and Accountability.195 It offers a twofold certification procedure. Firstly, Self-Certification: “An organization claiming compliance with the Code shall conduct an annual Self-Certification and confirm the successful results of this Certification to the CIF in order to receive authorization to use the “Certification Mark” for the following year.”196 Secondly, an organization may “opt for an Independent Certification performed by a Certification Body approved by the CIF.”197 This results in receiving the “Independent Certification Mark” which is similarly valid one year. According to the preamble of the CoP, CIF will “spot check and audit Self-Certifications as well as investigate any formal complaint of non-compliance against an organization claiming compliance with the Code.”198

191 See the website of CIF <http://cloudindustryforum.org/>, accessed 11 May 2014.
195 CIF CoP, Section A, B and C respectively.
196 CIF CoP, preamble.
197 Ibid.
198 Ibid.
CIF has authority to suspend or terminate the Certification Mark in case of non-conformity with the CoP or in case of finding a false declaration of compliance.¹⁹⁹

As mentioned, the CoP enforces three main principles. Firstly, the CoP highlights the principle of transparency. Under this module, “organizations complying with the CoP shall conduct themselves in an open and transparent manner which facilitates rational decision-making and management by purchasers of their services.” CoP highlights that it does not work as a pre-made judgement how the service provider should act, but only helps to ensure that essential information is provided to the end users.²⁰⁰ Transparency involves two categories of information: 1) information for public disclosure and 2) information for contracting disclosure. The former relates to information readily available on the provider’s website, e.g. compliance with the CIF CoP, corporate identity.²⁰¹ The latter specifically involves the acceptance of non-negotiable terms via the provider’s website.²⁰² Section A.2 of the CoP provides that information must be provided to the customer prior to signing the contract and by “means of disclosure on the organization’s website, by hyperlinked reference in the organization’s contractual terms and conditions, or in any other way.” It is appropriate to ask what this kind of setting adds to the existing understanding of the term “transparency.” The “Transparency” subdivision of the CoP provides rather ambiguous guidelines, e.g. under A.2.1 (“Commercial Terms”) the CoP foresees that the basis for termination of the contract must be provided with the terms and conditions. Clearly, such a formulation does not add anything to the openness and transparency of the T&Cs of the provider because all of the six cloud service providers already include a ground for termination. Section A.2.4 sub-indent (2) states the obligation to retrieve data in case of customer migrating to another cloud during the execution of the contract.²⁰³ Section A.2.8 sets the scene for provisions for service continuity. Again, the section only asks for “overview of measures … to provide for service continuity including protection against data loss.” The language of the sections provided in the section of “Transparency” are vague and require the service providers to give only general information in the ToS, consequently not

¹⁹⁹ CIF CoP, preamble.
²⁰⁰ CoP, A.
²⁰¹ CoP, A.1, A.1.1 and A.1.2.
²⁰² CoP, A.2.
²⁰³ CoP, A.2.4.
requiring the providers to meet any new criteria, but only set down the existing transparency requirements down in an obscure manner. Seemingly, the CIF has opted to be open for more clients, rather than truly providing a challenging threshold for the providers to meet to actually be “championing transparency” and a trustworthy assurance seal for the consumers.

Secondly, the CoP highlights the importance of “Capability” which is the second pillar of the CIF. Capability refers to the “ability of an organization to perform essential management functions, as demonstrated by having in place auditable documented management systems.” Section B of the CoP further sets the minimum requirements of “Capability” which include “written policies and procedures, specific individuals assigned with relevant responsibilities and appropriate training and awareness programs.” Section B highlights that depending on the size of the provider, certification under relevant standards of ISO and IEC may be desirable for an organization. Furthermore, for smaller organizations which do not consider such certifications appropriate, CIF “may in the future develop prototype management system documentation for the required areas.”

Thirdly, the CoP highlights the importance of accountability. Accountability only covers the service provider’s actions under the CoP, providing that “organizations which assert that they are complying with the Code shall be accountable for their compliance with the CoP and for their behaviour with customers.” Accountability forces organizations to be compliant with the CoP and to implement “formal procedures for complaint resolution within the organization itself” and show “willingness to agree to binding arbitration in local courts for the settlement of disputes.” Another side of the accountability coin is being compliant to the CoP during the one year period after the grant of the Certification Mark. To achieve this, section C.1 provides that potential non-compliance with the CoP “may be brought

---

204 CoP, B. Section B also highlights that these requirements are “similar, but less onerous than full management standards like ISO 9001, ISO/IEC 27001 and ISO/IEC 20000-1. “Meaning that the “Capabilities” are in some cases lower than set by the ISO and IEC.
205 Ibid.
207 CoP, B.
208 CoP, C.
209 CoP, C.2.
to the attention of the CIF in two ways: as a result of customer or whistle-blower complaints to the CIF and/or as a result of spot check and random audits conducted by the CIF itself or its appointed agents.” Furthermore, the organization is obliged to maintain auditable records to demonstrate its compliance for a minimum of 14 months.

Contrary to the guidelines about transparency, accountability rules of the CoP are specific and provide detailed provisions about what accountability means for a company. This includes forming an effective complaint-settling body and keeping auditable records to demonstrate compliance. This is important for a customer because in essence, accountability means that in case of litigation, the company is equipped to give access to the relevant documents (possibly self-incriminating) it possesses and, possibly, helping to win a case for the customer.

4.1.2 Moving the Cloud Industry Forum Code of Practice’s principles to practice – Is Cloud Industry Forum the true champion of trust and transparency?

As aforementioned, UKFast and Dell are members of CIF. This sub-section takes a closer view on section A.2 (“Information for Contracting Disclosure) of the CoP and the T&Cs of Dell Boomi and UKFast. CoP provides eleven sections which link to transparency; five of these sections deal with data migration and security (see A.2.3, A.2.4, A.2.6, A.2.7 and A.2.8 of the CoP). Section A.2.1 is most stringently related to user remedies and provides the recipe for transparent commercial terms. Section A.2.1 highlights that the commercial terms must include a pricing policy; payment terms; contract length; termination basis, terms and conditions; renewal and amendment terms and process. Sadly, that is all the CIF requires from commercial terms, and in the mind of the author, this is insufficient. The commercial terms itself should follow examples from case-law or law (e.g. Annex I of the UTD) and state that grounds for termination have to be specific and akin. None of such rules are included in the CoP. Under such a vague construction, it is impossible to understand how CIF is advocating transparency if it does not provide any guidelines for implementation of these commercial terms.

---

210 CoP, C.1.
211 Ibid.
212 CIF members, see <http://cloudindustryforum.org/membership/members>, accessed 29 April 2014.
Subsequently, it should not be difficult to adhere to these transparency guidelines. Payment terms are represented in clause 6 of UKFast T&Cs\textsuperscript{213} and clause 3 of the Dell Boomi’s T&Cs.\textsuperscript{214} Termination clauses are also present in the T&Cs of both providers.\textsuperscript{215} Length of the contract is not specified in a generic contract such as the T&C, but is specified in an order form, because the service can be provided on a pay-as-you-go basis. Only the pricing policy faces small problems of transparency in the T&Cs. As is visible from the payment clause of UKFast,\textsuperscript{216} the pricing policy is not a part of the ToS, but a part of the Order Form, which under clause 1.16 of the T&Cs means “the Company's standard Order Form signed by the Customer relating to the Services to be provided by the Company to the Customer.” Dell Boomi’s T&Cs clause 3, similarly, does not provide specific information about the pricing policy, providing that “Prices for the Products, Software and Services shall be stated in the Order Documents or Service Documents issued by Dell …”\textsuperscript{217} Again, it is clear that the pricing rules are shifted from the T&Cs. To provide a comparison, Windows Azure’s pricing and payment clause similarly provides that “payments are

\begin{footnotesize}
\textsuperscript{213} Example clauses from UKFast T&C’s payment clause:

\texttt{“6. PAYMENTS}
\texttt{6.2 The Company reserves the right to vary all charges to the Customer with one month's notice but any such variation shall only take effect on the contract renewal date or the anniversary of the contract commencement date (whichever is the earlier).}
\texttt{6.4 All payments shall be due to the Company on presentation of invoice or as otherwise stated on the Order Form. All payments shall be sent to the Company's registered office as set out in Clause 1.9 above or such other address as may be notified in writing from time to time by the Company to the Customer.}
\texttt{6.6 All charges and tariffs are quoted exclusive of Value Added Tax.}
\texttt{6.7 The Company reserves the right to change payment terms and require deposits if the Customer is more than 30 days late in making payments during the term of the Agreement in addition to or in lieu of any other remedies set out in the Conditions or otherwise available at law or in equity.”}

\textsuperscript{214} Examples from Dell Boomi’s payment clause:

\texttt{“3. Ordering, Prices, Payment}
\texttt{3.2 Prices for the Products, Software or Services shall be stated in the Order Documents or Service Documents issued by Dell.}
\texttt{3.3 Payment for Products, Software or Services must be received by Dell prior to Dell shipping the Products or providing the Software or Services to Customer or, if agreed in writing, within the time period noted on the Order Documents, or if not noted, within 30 days from the date of the invoice. Payment shall be made to the account indicated by Dell (as may be amended from time to time.)}
\texttt{3.4 All payments made or to be made by Customer to Dell under this Agreement shall be made free of any restriction or condition and without any deduction or withholding (except to the extent required by law) on account of any other amount, whether by way of set-off or otherwise.}

\textsuperscript{215} Dell Boomi’s termination clause, see 3.3.3.2.1 above. UKFast’s termination clause, see section 11 of the T&Cs of UKFast.

\textsuperscript{216} UKFast’s payment clause (6.1): “All charges for the Services, as detailed in the Order Form, shall be paid by the Customer to the Company annually in advance unless otherwise agreed in writing between the Parties in the manner prescribed on the Order Form.”

\textsuperscript{217} Clause 2 of the Dell Boomi’s T&C provide that Order Document “means the quotation and/or the order confirmation and/or the invoice sent by Dell to Customer which describes the Products, Software and Services purchased by Customer under the Agreement as well as Prices, payment terms and other provisions.”
\end{footnotesize}
due and must be made according to the Offer Details for your Subscription.” Consequently, it can be concluded that such a practice is common in the business. Although, the question arises – if this is common in the practice, should not the providers who seemingly value transparency and trust provide a higher level of transparency than the common level in the branch? For example, Dropbox provides an extensive pricing policy, where it provides when and how will the customer be billed. Though, it is eminent that Dropbox has to have a translucent pricing policy, because it contracts to a larger amount of consumers than Dell Boomi or UKFast. Thus, some negotiation room is left for the businesses.

In total, the CIF’s CoP cannot be considered as championing transparency, because it provides insufficient demands for service providers to meet.

---

218 Dropbox’s “Billing” clause: The fees for your Premium Account will be billed from the date you elect, or convert to, a Premium Account and on each monthly or yearly renewal thereafter unless and until you cancel your account. Click on the link on your "Account" page to see the commencement date for your next renewal period. Dropbox will automatically bill your credit card each month or year on the calendar day corresponding to the commencement of your Premium Account. In the event your Premium Account began on a day not contained in a given month or year, Dropbox will bill your credit card on the last day of such month or year. For example, if your Premium Account began on January 31st, February 28th is the next time your credit card would be billed. You acknowledge that the amount billed each month or year may vary for reasons that include, differing amounts due to promotional offers, differing amounts due to changes in your account, or changes in the amount of applicable sales tax, and you authorize us to charge your credit card for such varying amounts. Dropbox may also periodically authorize your credit card in anticipation of account or related charges. All fees and charges are non-refundable and there are no refunds or credits for partially used periods….”
4.2 Cloud Security Alliance’s (CSA) Security, Trust & Assurance Registry (STAR) initiative

The Cloud Security Alliance (CSA) has launched the Security, Trust & Assurance Registry (STAR) initiative at the end of 2011. The CSA STAR “is the first step in improving transparency and assurance in the cloud.” The objective and mission of CSA STAR are improving trust in the cloud and ICT market by offering transparency and assurance. Thus, like CIF, CSA is a tool for enhancing transparency in the cloud environment. But, does it also aim to enhance the remedial situation?

Dropbox, Google, Microsoft and Salesforce.com are all corporate members of the CSA. But, only Windows Azure is a member of the CSA STAR. All four of the CSA members are headquartered in the U.S and none of them is a member of the CIF at the same time as being a member of CSA. Similarly, CIF members UKFast and Dell are neither members of the CSA, nor CSA STAR.

The CSA STAR is a publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. The STAR certification system has three layers. First layer is the self-assessment, which is a publication of a due diligence self-assessment based on CSA Consensus Assessment Initiative Questionnaire and/or Cloud Control Matrix. Second layer is third-party assessment-based certification. It is a publication of a third party assessment based on Cloud Control Matrix and ISO 27001 or AICPA SOC2. The third and the most stringent assurance is continuous monitoring-based certification, which comprises of results of security property

---

220 Ibid.
221 Dropbox is a very recent member of CSA, the news about this was published on the 24th of April 2014, see <https://blog.cloudsecurityalliance.org/2014/04/23/dropbox-joins-the-cloud-security-alliance/> accessed 29 May 2014.
223 See the STAR registry entries <https://cloudsecurityalliance.org/star/#star_d> accessed 22 June 2014.
224 See <https://cloudsecurityalliance.org/star> accessed 29 May 2014.
226 Ibid.
monitoring, based on Cloud Trust Protocol.\textsuperscript{227} CSA STAR Certification assessment is based on ISO/IEC 27001:2005 (information security management system standard).\textsuperscript{228}

Besides the extravagant introduction to the STAR initiative, the webpage of CSA STAR does not provide information how the initiative actually works to enhance transparency. It seems that transparency is seen as a first step towards an efficient security assurance and transparency means only the publication of the results of a due diligence self-assessment based on CSA Consensus Assessment Initiative (CAI) Questionnaire and/or Cloud Control Matrix (CCM).\textsuperscript{229} Thus, transparency is seen from a different angle than in the case of CIF, where transparency directly means the provision of a more transparent standard terms to improve the remedial situation.

Under FAQ, the necessity to launch the STAR initiative is described by the CSA. It provides that “CSA believes that encouraging transparency and positive competition among cloud providers, with security as a market differentiator, is the right way to think about security in our computer systems. In these early days of cloud adoption, voluntary self-regulation of cloud providers is preferable to heavy-handed governmental regulation.” Thus, the usual incentive for self-regulation is explicitly conveyed – aversion of government regulation. It is also evident that transparency is not defined in the context of a contract assurance, but in the milieu of a security assurance.

In total, CSA STAR is an important security assurance provider, but it does not aim to improve the remedial situation between a cloud service provider and customers. Although security is one of the top risks related to the cloud\textsuperscript{230}, CSA STAR employs the branch standard ISO/IEC 27001:2005, while not even enforcing the 2013 version of the standard.

\textsuperscript{227} Information about Cloud Trust Protocol: \url{https://cloudsecurityalliance.org/research/ctp/} accessed 29 May 2014.
\textsuperscript{228} T&Cs of CSA STAR: \url{https://cloudsecurityalliance.org/star/#_terms} accessed 29 May 2014.
\textsuperscript{229} See supra note 219.
\textsuperscript{230} See J. Lansing et al., “Cloud Service Certifications: Measuring Consumers’ Preferences for Assurances”, p 5.
4.3 The Adverse case of TRUSTe

Current section provides an examples of what are the results of a lenient soft-law initiative. The author provides a brief look at TRUSTe’s privacy seal.

Dropbox’s Privacy Policy clause 10 provides that “Dropbox has received TRUSTe’s Privacy Seal signifying that this privacy statement and our practices have been reviewed by TRUSTe for compliance with TRUSTe’s program requirements including transparency, accountability and choice regarding the collection and use of your personal information.”231 According to the client list of TRUSTe, Salesforce.com is also a member of TRUSTe.232

TRUSTe’s website promotes itself as being the “leading global Data Privacy Management Company” who “powers trust in the data economy by enabling businesses to safely collect and use customer data across web, mobile, cloud and advertising channels.” The website also highlights that “more than 5,000 companies worldwide, including Apple, Disney, eBay, Forbes, LinkedIn and Oracle rely on our Data Privacy Management platform and globally recognized Certified Privacy Seal to protect / enhance their brand, drive user engagement and minimize compliance risk.”233

The TRUSTe Cloud solution provides businesses a service which is meant to “establish trust of Your cloud platform” by examining the privacy policy of the cloud provider and assessing the cloud platform’s data collection practices. According to TRUSTe, their service enables a cloud provider to reduce costs by implementing data controls and TRUSTe’s dispute resolution service for privacy matters.234

---

231 Under the same clause, the Privacy Policy properly highlights the accessibility of the complaint procedure: “If you have questions regarding this statement, you should first contact us at privacy@dropbox.com. If you do not receive acknowledgement of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe at http://www.truste.org/consumers/watchdog_complaint.php, by fax at 415-520-3420, or by mail to TRUSTe Safe Harbor Compliance Dept., click for mailing address. The TRUSTe dispute resolution process is only available in English.”
TRUSTe provides a Dispute Resolution Program, which “lets users hold TRUSTe clients accountable.”\textsuperscript{235} The Dispute Resolution Program is an online tool that allows users to report violations of the privacy statement and other privacy issues online.\textsuperscript{236}

According to TRUSTe, the Privacy Seal of TRUSTe is a sign of a fact that a “company operating that property has met the comprehensive privacy certification requirements established by TRUSTe.”\textsuperscript{237}

Looking at the website of TRUSTe, one cannot seem to ask if everything is really that perfect. Benjamin Edelman examined the TRUSTe’s Privacy Seal in 2009 and demonstrated that sites certified by TRUSTe are more than twice as likely to be untrustworthy as uncertified sites.\textsuperscript{238} The empirical study conducted by Edelman shows that only 94.6\% of the TRUSTed sites are trustworthy while 97.5\% of the non-TRUSTe sites are trustworthy.\textsuperscript{239} Clearly, this raises a serious question on the validity of the whole TRUSTe system and is a red light towards all assurance seals or “trust” certification providers. As Edelman said in 2006, if somebody says “you can trust me”, a person has to be extra cautious.\textsuperscript{240} Providing false trust is even more dangerous than not providing trust at all, therefore the Privacy Seal of TRUSTe provides a good example of the underlying dangers with the trust assurances.

\textsuperscript{235} TRUSTe’s Dispute Resolution Program \url{http://www.truste.com/consumer-privacy/dispute-resolution/} accessed 29 May 2014.
\textsuperscript{236} Dispute Resolution form, available at \url{https://feedback-form.truste.com/watchdog/request} accessed 29 May 2014.
\textsuperscript{237} See “What does the TRUSTe Seal Mean?” \url{http://www.truste.com/consumer-privacy/} accessed 29 May 2014.
\textsuperscript{239} Ibid, p 5.
4.4 Assurance seals – Sufficient Ameliorate for the Remedial Situation?

The field of trust assurances is wide and they mainly focus on security and privacy. Research conducted by many authors has shown that contract (and thus the remedial situation) is an important assurance, although privacy and security stand as the most important assurances for customers. There are many trust certificates for cloud providers and this thesis has focused on only three of them – Cloud Industry Forum, Cloud Security Alliance Security, Trust & Assurance Registry (STAR) and TRUSTe. Although a welcomed sight for the cloud industry, sadly, the soft law initiatives do not sufficiently improve the remedial situation in favour of the consumers/SMEs to achieve contractual balance.

The fourth chapter mainly emphasizes the CIF’s Code of Practice, because it is an initiative which explicitly seeks to improve the contractual balance through the implementation of transparent standard terms. Although having high expectations towards such a transparency enhancing tool, the CoP does not require the service providers to do more than present a pricing policy, payment terms, duration of the contract and a basis for termination in its T&Cs. In the opinion of the author, such a transparency block does not ask the certified companies enough and the threshold to meet the “transparency” criteria set by the CoP are low. Thus, it proves to be an inefficient tool for the improvement of the remedial situation. The requirements of transparency do not even allow to make a proper comparison with CIF certified providers UKFast (although UKFast’s T&Cs can be considered less severe than Dropbox’s, see 3.6 above) and Dell (which received the fewest reprimands, see 3.6 above) with the other non-certified members, due to the low threshold to meet the transparency principle under CIF’s CoP. Although the two providers employ a more balanced remedial situation than their comparative provider in their service model (Dropbox and Salesforce.com, respectively), this cannot automatically be accounted to the CIF’s certification due to a small sample group.

On the other hand, CIF cannot be considered as a failed initiative, because transparency is only one of the pillars of CIF (although the main one). CIF has specific rules about accountability and in the opinion of the author, CIF should be considered as an accountability tool, rather than a tool to enhance transparency.
CSA STAR takes another angle to the term transparency. Being a security assurance, it sees transparency as a publication of a due diligence report about the security measures of a cloud contract. Thus, it is not a tool to improve the remedial situation. Nevertheless, the CSA STAR asks its registrants to employ an industry standard of security techniques of 2005\(^{241}\), while the revised 2013 standard in the field exists.

Assurance seals are a necessary part of the electronic commerce which’s success is largely dependent on trust. As this chapter has shown through the writings of B. Edelman, TRUSTe’s privacy assurance encounters problems of trustworthiness and its seal is therefore undermined. An assurance seal is supposed be a signal to consumers that a website or service is more trustworthy than a competitor who has not acquired the seal. If this assumption proves out to be reversed, the untrustworthy sites with the assurance seals strongly undermine the honest members of an assurance seal and the situation is to the detriment of the consumers/customers.

In total, the analysed soft-law initiatives fail to improve the remedial situation of the cloud service providers. For these initiatives to be effective, they should employ a stricter set of requirements and monitor the behaviour of the companies who have received the certifications. As providers of assurances, they aim to make the life easier to a customer who should be able to make a decision who to contract with on the basis of these assurances. Regardless of the negative example provided by TRUSTe, experiments have shown that assurances help to make contracting decisions.\(^{242}\) Thus, it is important that such soft-law initiatives would not provide false trust.


\(^{242}\) See supra note 182.
5. Conclusion

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything — from computing power to computing infrastructure, applications, business processes to personal collaboration — can be delivered to users as a service wherever and whenever needed.\textsuperscript{243} It is a desired technological solution which simplifies the life of consumers and businesses. Also, it is cost-efficient, because the payment is made for actual usage, the business does not need to acquire computing power or storage space according to the peak demand, thus saving resources.\textsuperscript{244}

The thesis focused on all three cloud service models – IaaS, PaaS and SaaS, having a sample of two providers per service model. The thesis discusses the characteristics of a cloud contract, which can be described as being an imbalanced contract due to the lack of negotiation power on part of the customers (consumers and SMEs). The principle of freedom of contract allows the drafting of one-sided contract terms which, undoubtedly, influence the remedial situation to the detriment of the customers. Thus, where there is inequality of bargaining power, the weaker party requires more protection. Such a way of thinking has been accepted for consumers, however it is not omnipresent for SMEs, who also suffer from inequality of bargaining power.

The cloud contract is a “click-through contract” which aggravates the contracting situation for the customers. Click-wrap agreements are electronic agreements where the agreement is located on the same page as the “signature button.” The mean length of the standard terms presented by the providers with the factor that the contract is offered on a take-it-or-leave-it basis means that the “I agree” button will mostly be clicked without the contract terms actually being read. This thesis analysed what are the consequences in terms of the remedial situation after consumers and SMEs make the click. Although standard form contracts may be a practical method of contracting, in the current state, where the design of such contract are meant to deter people from reading them, the feasibility of standard


form contracts should not be taken for granted. Presently, the contracting situation is distorted from the start.

The thesis undertook to analyse the remedial situation in cloud contracts and asked if it could be considered an effective one. For this, the author analysed the T&Cs of six cloud service providers through the lens of the effectiveness criteria and consumer protection law, which provides a shield of protection against unfair terms. The criteria of effectiveness enable to provide clear indications whether the remedial situation can be considered balanced or not. The criteria of effectiveness, thus, represent a list of barriers set by the providers to seek an effective remedy. Such barriers are – time (time frame to initiate proceedings, enforcing an overlong curing period), costs (jurisdiction clauses and not providing refunds in case of termination), transparency (hidden terms, vague termination clauses and whole agreement clauses) and clear-cut cases of abuse (modification and variation clauses, assignment clauses and clauses which transfer the provider’s obligations to the customer). Consequently, the remedial situation is described through different impediments which all influence seeking redress in a hypothetical case of dispute. If none of these barriers exist, the remedial situation can be considered balanced – similar remedial possibilities are provided to both of the parties of the contract. Sadly, none of the six service providers included in the analysis pass the effectiveness criteria and every one of them place barriers to seek remedies for customers (see 3.6 above). Thus, the remedial situation at its current state must be considered imbalanced. The analysis aims to highlight the need for a change to the benefit to the consumers and SMEs, because it would be a mutually beneficial situation. Although the providers face a threat of more litigation initiated against them when the remedial situation is balanced, it would attract more customers and more subscriptions means more revenue for the cloud providers.

As the remedial situation is also analysed through the prism of Community law in the field of consumer protection, the analysis focuses on unfair terms which would not bind the consumer. Thus, the analysis concluded that the termination clauses of Google Apps for Business, Dropbox and Windows Azure could be considered unfair under sub-indent (q) of Annex I of the Unfair Terms Directive (93/13/EEC, hereinafter UTD) which deems a standard term unfair if it excludes or hinders the consumers’ right to take legal action or exercise any other legal remedy. Jurisdiction
clauses of all providers could possibly also be reproached under sub-indent (q) of Annex I of the UTD when they confer jurisdiction away from the domicile of the consumer. The consumers are shielded against such jurisdiction clauses under the Council Regulation (EC) No 44/2001 which results that consumers cannot be sued elsewhere than the Member State where the consumer is domiciled. Dropbox’s modification clause is considered unfair under sub-indent (j) of Annex I of the UTD, because it enables the service provider to alter the terms of the contract unilaterally without a valid specified in the contract. Also, the variation clause of Dropbox is considered unfair under sub-indent (k) of Annex I of the UTD because it enables the service provider to alter unilaterally, without a valid reason, any characteristics of the service provided. The assignment clauses of Dropbox, Windows Azure and UKFast are considered unfair in the analysis under sub-indent (p) of Annex I of the UTD since it gives the service provider the possibility of transferring his rights and obligations under the contract without the consumer’s agreement and the transference may serve to reduce the guarantees for the consumer.

The thesis also analyses the consumer protection laws of Estonia and UK to provide a comparative approach. These sections mainly aim to provide differences in the policy decisions of consumer protection, where in Estonian law, the SMEs are better protection against the unfair terms in a B2B contract where the UK law has taken a much limited approach. As the thesis argues that the rationale to protect SMEs against the cloud service providers with the superior bargaining power, the approach taken by Estonian law is preferred in the eyes of the author.

Lastly, the author analysed soft-law initiatives in the cloud context to see if they improve the current remedial situation in favour of the consumers/SMEs and introduce balance. The fourth chapter analysed the initiatives of Cloud Industry Forum, Cloud Security Alliance Security, Trust & Assurance Registry and TRUSTe. Although a welcomed sight for the industry, the soft law initiatives analysed do not sufficiently improve the remedial situation in favour of the consumers/SMEs to achieve contractual balance. Although Cloud Industry Forum and Cloud Security Alliance Security, Trust & Assurance Registry highlight the importance of transparency, neither of them foresee high enough demands for the service providers to meet. Cloud Security Alliance Security, Trust & Assurance
Registry does not aim to increase transparency in the T&Cs, but asks the service providers to publish a due diligence report about the security measures of a company. Cloud Industry Forum, on the other hand, explicitly aims to provide transparent T&Cs, and thus seek to enhance the remedial situation. However, the CIF’s Code of Practice only asks the providers to present a pricing policy, payment terms, duration of the contract and a basis for termination in its T&Cs. These obligations are considered too lenient for the service providers, thus, keeping the door open to a large number of registrations on behalf of the providers and not achieving the set goals about transparency. The negative case of TRUSTe is meant to issue a warning against the trust assurances. Trust assurances are seen as a guarantee, a sign that a certified cloud provider is more trustworthy than a competitor that is not certified. As in the case of TRUSTe, the empirical study conducted by B. Edelman showed that TRUSTe-certified websites were less trustworthy than non-certified providers. It is a red light towards all assurance seals and providing false trust is highly reprehensible.
Bibliography

Books

Articles

83


**Legislation**


13. The Unfair Terms in Consumer Contracts Regulations (UK), 1999

**Case-law**

**European Court of Justice**

1. Case 144/99 *Commission of the European Communities v Kingdom of the Netherlands*, [2001].
4. Joined cases 240/98 to 244/98 *Océano Grupo Editorial SA v Roció Murciano Quintero and Salvat Editores SA v José M. Sánchez Alcón Prades, José Luis Copano Badillo, Mohammed Berroane and Emilio Viñas Feliú*, [2000].
5. Joined cases 541/99 and 542/99 *Cape Snc v Idealservice Srl and Idealservice MN RE Sas v OMAI Srl*, [2001].

**From the United Kingdom**

1. *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582.

**From Estonia**

1. Civil Chamber of the Supreme Court of the Republic of Estonia, Case No 3-2-1-88-04.

**From the U.S**


**Soft law**

1. Cloud Industry Forum’s Code of Practice, version 6.1


86


Standard form contracts


2. Dropbox <https://www.dropbox.com/privacy#terms> (only the latest version provided)


Internet websites


34. Website of TRUSTe <http://www.truste.com/about-TRUSTe/>.

35. Website of UKFast <http://www.ukfast.co.uk/>. 