André Agreira (001244)

Cloud Computing and European Union Law:

An analysis of "standard" terms in Cloud Computing Agreements

Dissertation to obtain a Master's Degree in Law, in the specialty of in International and European Law

Professor:

Dr Francisco Pereira Coutinho, Professor at Nova School of Law

April 2020

Plagiarism Statement

I declare that I am the sole author of this dissertation, which is based on my research on the matter. All other sources used in its preparation have been duly referenced. I am aware that the use of works of third parties unless duly identified amounts to an ethical and disciplinary failure.

André de Caria Agreira

Munich, 18 December 2020

To my parents and sister for their unconditional encouragement and kindness,

To Prof. Dr. Francisco Pereira Coutinho for his insightful feedback and direction,

To all former colleagues at BHO Legal for their valuable insights and patience,

Especially to Dr. Baumann for his continuous guidance and inspiration,

To Rebecca for giving me the motivation and support to see this through,

To my friends for their unwavering support and care.

List of Abbreviations and Acronyms

A29WP	Article 29 Working Party
AG	Advocate General
AUP	Acceptable Use Policy
BCR	Business Corporate Rules
CJEU	Court of Justice of the European Union
CRD	Consumer Rights Directive
CRM	customer relationship management
CSP	Cloud Service Provider
DCD	Digital Content Directive
DoC	US Department of Commerce
DPA	Data Protection Authority
DPD	Data Protection Directive
DPO	Data Protection Officer
DSP	Digital Service Providers
EC	European Commission
EC2	Elastic Compute Cloud
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ERP	Enterprise Resource Planning
EU	European Union
EUCFR	Charter of Fundamental Rights of the European Union
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
IoT	Internet of Things
M2M	Machine-to-Machine
MS	Member State
NIS	Network and Information Systems
OTT	Over The Top

PaaS	Platform as a Service
PDA	Personal Digital Assistant
PII	personally identifiable information
SaaS	Software as a Service
SCC	Standard Contractual Clauses
SLA	Service Level Agreement
TEU	Treaty on the European Union
TFEU	Treaty on Functioning of the European Union
ToS	Terms of Service
UCTD	Unfair Contract Terms Directive
US	United States
VOIP	Voice over IP

This thesis contains a total of 185.558 characters

KEYWORDS: cloud computing, cloud service provider, data protection, data integrity, cloud contracts, terms of service, SLA.

ABSTRACT: As of today, one of the main obstacles to the transversal adoption of Cloud Computing by companies across the EU is still the lack of knowledge and the apparent risks associated to this technology; however, the European Commission has once again stressed its importance for the future of the EU. As such, this thesis provides a summary of the socio-economic relevance of cloud computing, as well as an overview of the fragmented the legal framework applicable to Cloud Service Providers in the EU. This thesis finally examines the adequacy and evolution of the terms of service provided by several cloud service providers, including their enforceability towards EU consumers, as well as the next steps to achieve a more competitive and transparent cloud market.

PALAVRAS-CHAVE: cloud computing, prestador de serviços de cloud computing, proteção de dados, integridade de dados, contratos de cloud computing, termos de serviço, SLA.

RESUMO: Actualmente, um dos principais obstáculos à adoção transversal do cloud computing por empresas na UE prende-se com a falta de conhecimento relativamente aos serviços de cloud computing e aos riscos aparentes associados a essa tecnologia; apesar disso, a Comissão Europeia voltou a salientar a importância do cloud computing para o futuro da UE. Como tal, esta tese fornece um resumo da relevância socio-económica do cloud computing, bem como uma visão geral das múltiplas normas jurídicas aplicável aos provedores de serviços de cloud computing na UE. Finalmente, a tese examina a adequação e evolução dos termos de serviço fornecidos por vários provedores de serviços de cloud computing, incluindo sua aplicabilidade em relação aos consumidores da UE, bem como os próximos passos para alcançar um mercado em nuvem mais competitivo e transparente.

Contents

PART 1 - INTRODUCTION

"We're on the brink of a big change: technological, social, economic. People everywhere get it – in Europe and across the world. Many of these national leaders get it. Do you?"[1]

1.1 Proposition and scope of the analysis

My thesis aims to clarify some of the myths surrounding cloud computing, especially those concerning the new European data protection framework[2] and the upcoming proposals which aim to revolutionise electronic communications and e-commerce.[3] According to Eurostat's data, the significant factors limiting the adoption of cloud computing are the risk of security breaches, the lack or insufficient knowledge/expertise, the high cost of cloud computing services, the uncertainty concerning data location, legal jurisdiction in the event of disputes and of the applicable law. As evidenced below, most of these issues have been, to some extent, tackled and solved by the applicable legal framework and by cloud computing contracts, as well as by soft law instruments.[4]

I chose this topic due to its general importance of the topic, duly evidenced by both the amounts it generates (as per section 2.5.3) and its continuously growing adoption rates, but also due to a desire to fully understand what are the limitations, pitfalls and dangers of relying on cloud computing services and the standard practices in this sector.

---

1 Neelie Kroes, European Commission Vice-President for the Digital Agenda, Speech at the InfoPoverty World Summit, 10 April 2014.

2 See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

3 See COM (2017) 10 final, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) and COM (2015) 634 final, Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, respectively.

4 According to Eurostat's data, the major factors limiting the adoption of cloud computing are the risk of security breaches, the lack or insufficient knowledge/expertise, the high cost of cloud computing services, the uncertainty concerning data location, legal jurisdiction in the event of disputes and of the applicable law. However, as evidenced below, most of these issues have been, to some extent, tackled and solved by the applicable legal framework and by cloud computing contracts, as well as by soft law instruments. As per Eurostat: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Factors_limiting_enterprises.E2.80.99_use_of_cloud_computing_.282014_survey.29 (last accessed on 26/04/2020).

Accordingly, this thesis will provide a brief overview of the European legislative texts affecting cloud computing, while focusing on the conditions set forth in the contracts between businesses and the customers relying on it.

I will commence my thesis by defining the central concept of this thesis – *i.e.* cloud computing – and explain the diverse models of cloud computing services. Subsequently, I will indicate the standard parties in a legal relation in cloud computing. After such introduction, I will demonstrate the significance of cloud computing in the world market, its importance in the current corporate scenario, not only supported by the amounts it generates, but also by the advantages it creates for enterprises using these services, as well as by the increasing demand for cloud computing supported applications. Subsequently, I shall analyse the legal framework of cloud computing across the European Union (EU), dedicating specific attention to the data protection framework. I will then focus on commercial aspects and evaluate available cloud computing contracts and the typical provisions included by a Cloud Service Provider (hereafter designated as "CSP"), to ascertain a pattern or, where relevant, to highlight positive and innovative practices being undertaken. Lastly, I will present my findings and conclusions, with the aim of increasing user trust on cloud computing and further expanding its adoption.

PART 2 – GENERAL BACKGROUND

2.1 The History of Cloud Computing

Historically, the first allusion to cloud computing was made in 1961, by computer scientist John McCarthy. At that time, McCarthy indicated that "*computing may someday be organized as a public utility just as the telephone system is a public utility (...). The computer utility could become the basis of a new and important industry*"[5].

A few years later, in 1963, JCR Licklider, which spent the 1960's developing ARPANET, the predecessor to internet, introduced the idea of a globally accessible network, which would allow an individual to access computer programs and data from any location, an idea that closely relates to the present notion of cloud computing. The same author also suggested that, in the future, there would be an "intergalactic computer network",[6] anticipating the introduction of cloud computing and big data in the following years.

The succeeding decades brought forward many developments, namely the first e-mail (1971), the release of the World Wide Web for general use (1991) and the introduction of the concept of grid computing (1998), by Ian Foster and Carl Kesselman,[7] in which, tracing the analogy from the electric power grid, the users could plug in and use the capabilities of computers from various locations to reach an objective. The first actual recorded reference to the term "cloud computing" can be traced back to 1996.[8]

It was not until 1999 that, in a small San Francisco apartment, cloud computing gave its first steps by the hand of Salesforce.com[9], which was the first site ever to provide business applications from a typical website. This endeavour was only possible due to the increased availability of network broadband. In this sense, the appearance of Salesforce was the first of four events that have defined the cloud industry, as it came to be known.

---

[5] Speech at the MIT Centennial in 1961, cited in Garfinkel, Simson L., "Architects of the Information Society, Thirty-Five Years of the Laboratory for Computer Science at MIT", ed. Hal Abelson, MIT Press, 1999, p.1.

[6] Licklider, J. C. R., "Memorandum For: Members and Affiliates of the Intergalactic Computer Network", Advanced Research Projects Agency (ARPA), 1963; Available at: http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network (last accessed on 26/04/2020).

[7] Foster, Ian, and Kesselman, Carl eds., "The Grid 2: Blueprint for a New Computing Infrastructure", 2nd edition, Elsevier., 2003, pp. 1-11 and 37-63.

[8] See https://www.technologyreview.com/s/425970/who-coined-cloud-computing/ (last accessed on 26/04/2020).

[9] See https://www.salesforce.com/company/about-us/#1999 (last accessed on 26/04/2020).

Another historical milestone was the arrival of Amazon Web Services in 2002, which delivered cloud-based services such as storage, computation and human intelligence[10]. The next historical landmark took place in 2006 when Amazon introduced its second generation of cloud services – Elastic Compute Cloud (EC2) –, which allowed individuals and smaller companies to rent computing space to run their computer applications and to meet their data storage needs, thereby simplifying and broadening the access to cloud computing.

The last relevant milestone happened in 2009, with the unveiling of Google Apps, which introduced browser-based cloud enterprise applications, offering cheap and easily accessible applications for computers, smartphones, and tablets. Microsoft, with Windows Azure, and Apple, with iCloud, and other large companies have also presented their own Cloud platforms, which demonstrates that the shift towards the use of cloud computing is underway and will have a significant impact.

2.2 Defining Cloud Computing

The task of defining cloud computing is not simple, given that since its appearance many new innovative functions have been introduced and thus the definition has evolved. Also, cloud computing cannot be perceived as a single technological solution, but as a broader concept used to define a range of different technologies and applications. Thus, before presenting any concrete characterisation of this notion and since little consensus exists on the matter,[11] I will indicate the main characteristics usually associated with cloud computing, to be able to determine the concept with precision.

Accordingly, the most common characteristic of cloud computing is that is sold as an on-demand self-service; this is corroborated by the possibility of its users to request computer services (*interalia* e-mail, applications, network storage) automatically, without requiring human interaction with the service provider.

The second main feature is its broad network access, which means these capabilities are available over the network and can be accessed through standard applications by universal platforms as mobile phones, laptops and PDAs.

---

[10] Human Intelligence Tasks (commonly known as HITs) enable businesses to approach a large number of users to perform services that computers are still unable to do. Usually, companies will post tasks such as identifying performers, choosing pictures or writing products descriptions, *inter alia*.

[11] See Geelan, Jeremy, "Twenty One Experts Define Cloud Computing," Virtualization. August 2008. Electronic Magazine, 2009.

The third typical characteristic of cloud computing is the provision of resource pooling (or sharing), i.e. the provider's computing resources are combined to serve multiple consumers using a multi-tenant model, with various physical and virtual resources, which enable the creation of economies of scale. A particular word of caution concerning this third characteristic: even though most users will avail from resource pooling, not all cloud computing services will be provided as such (e.g. private clouds).

A fourth pivotal feature of cloud computing is its rapid elasticity, by which the services provided can be quickly and dynamically delivered in accordance to the user's needs. Finally, and relating to the aforementioned characteristic, the usage of cloud computing services can be measured, controlled and reported, thereby increasing the transparency of the used service. Therefore, a typical analogy has been traced between cloud computing services and utilities, since, in both services, consumers are charged according to their usage of the service. This ultimately leads to an optimisation of resources and efficiency gains.

The abovementioned characteristics (on-demand service, network access, resource pooling, elasticity [or dynamism] and measured service) are not the single identifiers of cloud computing, nonetheless, they are the features that have been emphasised by the NIST[12], ITU[13] and the EU[14], as well as by experts[15].

For the purposes of this thesis, I considered the definition, as established by Bradshaw and Walden[16]:

> *"Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand. Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers. Charging, where present, is commonly on an access basis, often in proportion to the resources used."*

---

[12] As per the NIST definition: https://csrc.nist.gov/publications/detail/sp/800-145/final (last accessed on 26/04/2020)

[13] ITU, FG Cloud Technical Report Part 1, Geneva, 2012.

[14] "The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010", European Commission: https://ec.europa.eu/digital-single-market/en/news/future-cloud-computing-opportunities-european-cloud-computing-beyond-2010-expert-group-report (last accessed on 26/04/2020) and A29WP, "Opinion 05/2012 on Cloud Computing", WP 196, 2012.

[15] See MacVittie, Lori, "Cloud Computing: The Last Definition You'll Ever Need": https://devcentral.f5.com/articles/cloud-computing-the-last-definition-youll-ever-need#.U2OifqJx2GV last accessed on 26/04/2020). See also, lummer, Daryl. "Experts define cloud computing: can we get a little definition in our definitions.": http://blogs. gartner. com/daryl_plummer/2009/01/27/experts-definecloud-computing-can-we-get-a-little-definition-in-our-definitions (last accessed 26/04/2020).

[16] See further Bradshaw, Simon, Christopher Millard, and Ian Walden., "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services", Queen Mary University of London, School of Law Legal Studies Research Paper No. 63, 2010, p. 6.

This specific definition was selected since it includes the central features of cloud computing, while also considering virtualisation,[17] an important characteristic which contributes significantly to the rapid scalability of cloud infrastructure since virtual instances can be changed according to the customer's needs.

2.3 Categories and deployment models

As previously noted, cloud computing allows for numerous applications, which are designed to lodge users' specific requirements. As a consequence, the delivery of cloud computing may often depend on intricate, multi-layered arrangements between various providers and many permutations are possible. However, the bulk of these cloud services will fall into one or more of the following three service categories[18]:

I. Infrastructure as a Service (henceforth addressed as "IaaS") – in this category the Cloud Service Provider (from now on referred to as CSP) provides raw computing resources, such as storage, processing power or intra-cloud connectivity services, *inter alia*. In this service the user will usually not manage or control the resources underlying the cloud infrastructure, but will have control over the operating systems and deployed applications;

II. Platform as a Service (hereafter designated as "PaaS") – in this model the user can deploy, create and develop its own applications on the provider's platform over the network, which offers a high-level integrated environment. However, this model also has some restrictions; for instance, the type of software will have to be written in the provider's scalable systems,[19] which still occurs due to the lack of fully accepted standards for interoperability or data portability;

III. Software as a Service (hereafter referred as "SaaS") – the main service provided is special-purpose software, which is remotely accessible by the network and com-

[18] The segmentation of these service models has been advanced by the NIST in 2011 (see Mell, Peter and Grance, Tim, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, 2011, p. 2).
[19] One example of this is Google's App Engine, in which created applications will be written on the same scalable systems that power Google applications (see: https://cloud.google.com/products/app-engine/, (last accessed on 26/04/2020).

monly delivered to multiple users, on a usage-based pricing model, for example, the provision of Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) services, as well as email and web hosting.

According to the "2014 Priorities Europe"[20] report, elaborated by TechTarget, SaaS is the cloud service most companies use in Europe (44%). In addition, the move towards the cloud has led to the creation of other types of service categories such as AaaS[21] (Authentication as a Service), DaaS[22] ("Data as a Service"), InaaS[23] ("Information as a Service") and other new models[24]. A further deployment model is XaaS[25], which corresponds to everything/anything as a Service; its main advantage arises from a possible combination of previously separated cloud services into a single cloud, thereby promoting a flexible, tailor-made environment and increasing system integration (and consequently reducing overall integration costs).

On the other hand, besides these categories, cloud computing can also be divided into the following deployment models, according to the security restrictions envisioned by the cloud user:

I. Private cloud – the relevant infrastructure is operated for the benefit of a single user or a group of related entities. The user disposes of autonomy and control over the cloud structure and the associated data centre. However, this does not imply that private clouds are necessarily on premise, but merely that the infrastructure used is dedicated to the concerned customer;

II. Public cloud – in contrast with private clouds, the cloud infrastructure is shared by multiple users and a public cloud will usually use pooled share resources over a public network. These services can be free and some companies use them to storage non-sensitive content to make their operations more efficient.

III. Community cloud – a multi-tenant infrastructure that is shared, owned and usually operated on behalf of a specific group of users, with common computing concerns

---

[20] See http://docs.media.bitpipe.com/io_10x/io_102267/item_835374/2014%20Priorities%20Europe.pdf (last accessed on 26/04/2020).

[21] This type of cloud service contributes to a higher degree of security, by allowing users to track password usage, enforce strict password requirements and provide employees with a secure mechanism to log into diverse applications and web services remotely from the Cloud

[22] DaaS allows users to access data in a timely, safe and affordable way; large companies may storage data in one location and allow data to be used or modified by multiple users through a single update point, with the objective of reducing redundancy and associated costs.

[23] InaaS aims to process data into relevant information, as such, it provides users the ability to use standardized and secure methods to create, manage, exchange, and extract meaningful information from larger sources of data, in the desired format.

[24] Such as Communication as a Service (Caas), Monitoring as a Service (MaaS) and IT as a Service (ITaaS). See Rittinghouse, John W. and Ransome, James F., "Cloud Computing: Implementation, Management and Security", CRC Press, 2009, , pp. 30-32, 44-48 and 155-156, respectively.

[25] *Idem* pp. 156-157.

(for example regulatory compliance or audit/security/performance requirements), such as public bodies or the financial services industry. This model combines the economic benefits of a public cloud while maintaining a high level of privacy and security;

IV. Hybrid cloud – this model involves a combination of private and public cloud elements, allowing an organisation with a private cloud to cloud burst[26] processing services to a public cloud when the demand for computing capacity spikes. The advantage of this model is that an organisation will only pay for the required resources, however, security and compliance requirements should be considered before adopting it, since it could endanger sensitive information by bursting it to the public cloud.[27]

2.4 Parties in a Cloud Computing legal relation

Considering the complexity of cloud computing it will not be surprising to observe the existence of various parties to a cloud computing legal relationship.

Inexperienced customers may consider the cloud aggregator as the *de facto* cloud provider, since either they are not aware that services are provided using a first-tier cloud provider or because, in its dealings, the customer will only interact directly with the cloud aggregator. Such aggregator will often incorporate services provided by one or more cloud providers, which it will market as a sole product to its customers; thus, it will be simultaneously a cloud consumer and cloud provider. .

Nonetheless, in the scope of my analysis, I will focus on the cloud aggregator (or reseller), on the cloud provider (be it SaaS, IaaS or PaaS) and on the cloud user (i.e. the acquirer and the end user of the Cloud service(s)), despite the existence of other stakeholders in this business segment.[28] In addition to the entities mentioned in the preceding sentence, I will also address, in part III,[29] the concepts of controller and processor, when addressing the General Data Protection Regulation[30] (henceforth referred to as "**GDPR**"). The aforementioned definitions – aggre-

[26] See http://searchcloudcomputing.techtarget.com/definition/cloud-bursting (last accessed on 26/04/2020).
[27] See Millard, Christopher J., ed., "Cloud computing law", Oxford University Press, 2013, p. 5.
[28] Namely the cloud auditor, cloud carrier and tool providers, integrators, consultants, cloud end-users, cloud customers, etc..
[29] See section 3.2.1.
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

gator, provider and seller – will be of further importance in the upcoming chapters of this thesis, since the role of various parties will contribute to understanding who uses the underlying data and will enable to differentiate the data processor, data controller and the data subject.[31] Furthermore, one should note that aside from the rights specified by the applicable legislation,[32] the remaining rights/obligations of the parties will be established by the agreements concluded between them, which may change significantly, in view of the characteristics of the service being rendered.[33]

2.5 An overview of the current status of cloud computing: advantages, risks and market

This sub-chapter aims to provide a brief overview of the cloud computing so as to introduce the advantages arising from its use and the potential risks, as well as to demonstrate its global relevance and the amounts expected to be derived from it.

2.5.1 The advantages of the Cloud

The rapid adoption of cloud computing is the result of the competitive advantage it generates for both end users and businesses, which made it one of the most relevant innovations in recent years. Authors[34] indicate the following as cloud computing's main advantages:

a) **Scalability / Elasticity** – instances are automatically deployed when required; thus, the provision of service is elastic and can be scaled to meet the user's IT demands (i.e. data storage, web hosting or computing capabilities).

b) **Cost Efficiency** – "pay per use" and the access to resources on-demand, allows users to deal with unpredictable or temporary needs, without complex commitments

c) **Availability and reliability of service** – some Service Level Agreements[35] (also called SLA) provide availability rates up to 99,99%; in addition, renowned cloud pro-

[31] Idem.
[32] See Part 3.
[33] See Part 4.
[34] See Weinman, Joe, "Cloudonomics: The Business Value of Cloud Computing", John Wiley & Sons, 2012; also, Buyya, Rajkumar, James Broberg, and Andrzej M. Goscinski, eds., "Cloud computing: Principles and paradigms", Vol. 87, John Wiley & Sons, 2010; and op. cit in note 27.
[35] Service Level Agreements are addressed in section 4.3.4. For more information, please see Burnett, Rachel, "Outsourcing IT – The Legal Aspects", 2nd edition, Gower, 2009, pp. 59-74; Burnett, Rachel and Klinger, Paul, "Drafting

viders also have a number of failover mechanisms which allow a consistent and continuous service, in case a server fails.

d) **Location independence** – data and applications are available to users anywhere in the world; this promotes collaboration by allowing geographically scattered individuals to meet virtually and to work and share/use information in real time.

e) **Quick deployment and integration** – users can set up their systems in minutes and start working immediately and some providers may allow users to cherry-pick the services and applications for greater customization.

f) **Performance** – higher speed of computation since it relies on distributed architectures, which usually run on state of the art equipment; the geographically dispersed footprint of a cloud service also contributes to enhancing the end-user experience.

The above characteristics contribute to the two major selling points of the cloud: **productivity** and **innovation**. The idea that cloud computing fosters productivity and innovation is associated with the notion that the transition to the cloud is usually complemented by a refresh of technology and that such upgrade (i.e. use of cutting edge technology and applications) will leverage operational efficiency gains, promote the company's adaptability, and enable the company to venture into new markets.

2.5.2 Challenges to the adoption of Cloud Computing

Despite the benefits of cloud computing, a relevant number of risks and challenges arise from this new model of computing. Thus, it is prudent to analyse the potential issues associated with such technology to avoid them or, at least, to mitigate their risk of occurrence. Below, is presented a list of the potential risks typically associated with cloud computing:

a) **Security and privacy of data:** even though cloud providers present security standards and industry certifications,[36] a majority of potential cloud users[37] fear losing control over their data, namely due to the misuse of information by the provider or by

and Negotiation Computer Contracts", 2nd edition, Tottel Publishing, 2005, pp. 4000-404; Blokdijk, Gerard, "Service Level Agreement 100 Success Secrets", Emereo Publishing, 2008.

[36] *Inter alia* the ISO/IEC 27000's series; however, other standards are also used.

[37] In with the "Cloud Adoption Practices & Priorities Survey Report", in January 2015, 73% of the respondents indicated that security of data was one of the challenges holding back the adoption of cloud project; see Coles, Cameron et al., "Cloud Adoption Practices & Priorities Survey Report," Cloud Security Alliance, 2015: https://downloads.cloudsecurityalliance.org/initiatives/surveys/capp/Cloud_Adoption_Practices_Priorities_Survey_Final.pdf (last accessed on 26/04/2020).

third-parties, in the event of a cyber-attack. However, it should be noted that the security standards of cloud providers often go far beyond the degree of security a single company could maintain within their own ICT infrastructure.

b) **Legal uncertainty:** the provision of cross-border services, the use of data centres in diverse (including non-EU) locations and the uncertainty of the location of data are further major issues raised by users. The lack of knowledge regarding the legal jurisdiction and the underlying legal framework, regarding both data protection and access to data by intelligence agencies, are risks which need to be assessed and even mitigated before the adoption of cloud computing.

c) **Vendor lock-in and data portability:** lock-in refers to the risks associated with the overdependence on a provider's proprietary product or service, or the considerable cost of changing to a different provider; data portability[38] refers to the difficulties in the recovery of data and metadata in a format, which is easily accessible, readable and importable to other applications or service providers. Both issues are intrinsically connected and are especially relevant due to the lack of widely accepted standards and protocols, which can enable, support and assist in the replacement of a vendor or an application.

d) **Lack of Transparency:** many users are unaware how their CSPs structure of their procedures and practices, as well as whether they rely on subcontractors for the processing of data. Such may hamper users ensure compliance with data protection rules and increase the fear of losing control over its data.

e) **Ownership of data:** though ownership of data remains with the originating data owner, issues related to ownership of data generated in the Cloud still arise, as well as those relating to the use of user owned/generated content by CSPs.[39]

f) **Downtime:** users should assess any existing SLA thoroughly, namely the availability rates, the way those are calculated and any associated service credit scheme associated with them. Furthermore, users should be aware that services may be compromised if the users' own internet connections fail or are disrupted.

[38] At this point, the concept of data portability is used broadly, including application portability, interoperability and the recovery of data upon termination; these topics will be assessed in section 4.2.4 and 5; see also Buyya et. al, pp. 533-534 (op. cit. in note 34) and Ed Moyle, "Three Practices to Prevent Cloud Vendor Lock-In," Techtarget.com, 2013, https://searchcloudsecurity.techtarget.com/tip/Three-practices-to-prevent-cloud-vendor-lock-in (last accessed on 26/04/2020).

[39] For more information on this issue, please refer to Reed, Chris and Cunningham, Alan, "Ownership of Information in Clouds", in Cloud Computing Law, ed. Millard, C., Oxford University Press, 2013 pp. 142-164.

g) **Liability of the provider:** most providers only offer limited guarantees to their services and either exclude or cap their liability for data loss, corruption or service failure, which usually leads to users raising serious concerns about transferring business-critical data and applications into the Cloud.

In light of these challenges, the cloud computing community has taken noticeable steps to address them, as demonstrated by the emergence of security standards, *interalia* the ISO/IEC 27000's series, and, to a certain extent, by CSPs willingness to address concerns by European consumers and attempting to mitigate risks and update contractual terms.[40] Also, most cloud providers are already acquainted with the concerns of cloud customers and have addressed them effectively, by continually improving their infrastructures. These measures are commendable, however, further steps should be taken by industry and academia to ensure that legal uncertainty and concerns regarding data privacy and data integrity do not hamper the adoption of cloud services.

2.5.3 Brief overview of the market and a bridge to the future

After becoming widely available in the mid-2000s, cloud services' uptake followed the distribution pattern of general innovations:[41] it was initially perceived with some distrust, receiving some criticism from relevant figures in the IT world, declaring the notion to be merely "fashion driven" and "complete gibberish",[42] and others considered the service "a trap"[43], in addition to the risk presented above and others such as the lack of open standards and many associated legal issues.

Nonetheless, cloud computing still managed to gain momentum, and, in 2009, global revenues were expected to generate a total of 56.3 billion dollars, an increase of more than 20% over

[40] E.g. in the UK the Competition and Markets Authority comments led to the improvement of the terms in several cloud storage providers: https://www.gov.uk/government/news/cma-secures-better-deal-for-cloud-storage-users, (last accessed on 26/04/2020).

[41] As indicated by Etro, Frederico, "The Economics of Cloud Computing", IUP Journal of Managerial Economics, 2011, vol. 9, issue 2, pp. 7-22: "the introduction of new technologies has often created initial resistance (think of modern assembly lines), initial diffidence (think of early mobile phones), visionary ideas (think of Bill Gates' claims of bringing a PC in every house), a slow adoption at the beginning (even for electricity), with a mix of clear general benefits and specific costs (think of new energy sources), and finally a process of rapid and generalized adoption".

[42] In September 2008, Larry Ellison, former CEO of Oracle, stated that "[t]he interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do (…) The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane", see https://www.cnet.com/news/oracles-ellison-nails-cloud-computing (last accessed on 26/04/2020).

[43] Following the comments of Oracle's CEO, Larry Ellison, GNU founder, Richard Stallman, told the British newspaper "The Guardian" that cloud computing was "worse than stupidity: it's a marketing hype campaign", see https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman (last accessed on 26/04/2020).

the previous year.[44] Since then, new competitors have appeared from contiguous areas and used their expertise in managing large and cheap data centres to become relevant players. This has led to an increased confidence in the capabilities of cloud computing to grow.

In the European Union much importance has been given to this topic[45]; however the adoption of cloud computing services appears to be slightly slower than in the United States,[46] with only one in five EU companies reporting to use cloud computing services, a figure which can be explained by the perceived security risks associated with cloud computing, the lack of expertise and knowledge concerning contractual aspects, and the EU complex legal framework.[47]

However, the latest figures display an increase in the adoption of cloud computing services. Also, the emergence of value-added services, which have combined and increased the functionality of existing computing, storage and software services, have allowed such market to continue growing. Lastly, the recent entrance of further providers prepared to address the needs of both individuals and start-ups will likely foster competition and innovation in this market.

Thus, even though the figures provided by consultancy companies differ significantly[48], the overall figures present an exciting pattern. According to the figures of May 2017 the global cloud managed services market was expected to grow from over 27 Billion US Dollars in 2017 to over 53 Billion by 2022,[49] which further validates the economic relevance of cloud computing.

---

[44] As per the Gartner press release of March 26, 2009; however, one should consider that a major part of this amount included cloud-based advertising (59%), which is not an actual CC service, but was merely provided through the cloud, see http://www.gartner.com/newsroom/id/920712 (no longer accessible).

45 See COM(2012) 529 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe.

[46] Gartner announcement in 2012 on the potential inhibitors of cloud adoption in Europe, see http://www.gartner.com/newsroom/id/2032215 (no longer accessible). Also, one should not disregard the clear early mover advantages still held today by the US- based cloud services providers.

[47] Data by Eurostat on the use of cloud computing by enterprises, see http://goo.gl/pUD47I (last accessed on 26/04/2020). However, we note that the results differ substantially within the EU-area, with some states presenting cloud computing adoption rates above 30% (i.e Finland, Iceland, Italy, et. al.) and others rates below 10% (e.g. Greece, Bulgaria, Poland, *etc.*).

[48] For instance, see David Bradshaw et al., "Uptake of Cloud in Europe - Follow-up of IDC Study on Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-Up," Digital Agenda for Europe, 2014, http://goo.gl/BJ22xd (last accessed on 26/04/2020).

[49] As per the Markets and Markets report on the the Cloud Managed Services Market http://www.marketsandmarkets.com/Market-Reports/cloud-managed-service-market-195317068.html (last accessed on 26/04/2020).

PART 3 – LEGAL FRAMEWORK

As indicated above, the use of cloud computing raises complex legal challenges, resulting from the fact that the regulation of cloud computing within the EU covers diverse areas of law and significant efforts are required to be aware of the legal obligations arising from its use and to create the corresponding compliance instruments.

As indicated by Eurostat, one of the major concerns pertaining to cloud computing in the European area relates to data protection and data privacy.[50] Also, it is essential to note that, even though the terms data protection and data privacy are often used interchangeably, they are distinct, albeit they deeply connected and, at times, overlapping.[51] Additionally, other issues may also raise relevant legal questions from the use of cloud computing, namely those concerning vendor lock-in and data portability, liability of the provider and quality of service.

Bearing such in mind, this section will be dedicated to the analysis of the relevant primary and secondary sources of EU law, including relevant jurisprudence of the Court of Justice of the European Union (**CJEU**), where relevant, and their consequences on cloud computing. Furthermore, considering the entry into force of the General Data Protection Regulation (GDPR)[52] and of the Digital Content Directive (DCD),[53] as well as the proposal for an ePrivacy Regulation[54] , I shall also assess the alterations to be introduced and the effect that such may have on the cloud industry.

---

[50] See footnote 1.

[51] As per Gutwirth, Serge et al., "Reinventing Data Protection?", Springer, 2009. See also, Bygrave, Lee A., in "Privacy Protection in a Global Context – A Comparative Overview", in Scandinavian Studies in Law, vol. 47, 2004, p. 319–348.

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[53] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[54] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM (2017) 10 final.

3.1 Primary sources of EU Law

As De Hert and Gutwirth[55] refer data protection and data privacy are different, but complementary fundamental rights. According to the authors, a sharp distinction must be traced between these two concepts. Thus, while the first (i.e. data protection) provides the necessary instruments to ensure the protection of the data subject, namely its ability to enforce its rights concerning the processing of his/her personal data and to ensure processor's accountability, the latter (i.e. data privacy) stems from the right of individuals to protect their personal and familiar sphere, creating a "shield around the individual, (…) a zone of autonomy and liberty".[56]

In this context, it is relevant to notice that the Lisbon Treaty, which amended the two central treaties constituting the EU – the Treaty on the European Union ('TEU') and the Treaty on the Functioning of the European Union ('TFEU') –, promoted an important alteration to Article (Art.) 6 TEU. In this article, the EU recognised that the "rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union" (EUCFR) held the same legal value as the treaties and promoted the EU's accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms ('ECHR'). [57] The TFUE and the EUCFR will provide a framework to assess the impact of data protection and data privacy in cloud computing within the EU, since they establish data protection and data privacy as fundamental rights.

Accordingly, data protection is addressed in both Art. 16 TFEU and Art. 8 EUCFR, which reiterate that everyone has the right to the protection of its own personal data. In addition, Art. 8(2) EUCFR states that such data must be processed fairly and on the basis of the consent of the concerned person or some other legitimate basis, as provided by law. Conversely, the right to privacy is addressed in Art. 7 EUCFR and Art. 8 ECHR, which provides a general right to privacy, including the person, its family, home and correspondence. In light of this, one must recognise that the ECHR had a significant influence on the EU provisions on these matters and, the European texts, should, therefore, be interpreted taking into consideration such influence.

One of the most relevant legal texts on the data protection framework was Convention 108 of the Council of Europe, which has been signed by all EU Member States and by the EU in

[55] See De Hert, Paul and Gutwirth, Serge, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in Privacy and the criminal law, by Claes, Erik., Duff, Antony and Gutwirth, Serge (eds.), Intersentia, 2006, pp. 61-104.
[56] See footnote 51, Gutwirht, P [et al], page x (preface).
[57] Art. 6 TUE: "1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union (…). 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms."

1999. [58] The Convention was the first major element setting forth provisions pertaining to the protection of automatic processing of personal data, concerning scope, duties of the parties, quality and transfer of data, *inter alia*. Convention 108 remains open for signature by non-member States of the Council of Europe[59], which leads some entities to consider whether such instrument "could serve as a basis for promoting data protection at global level".[60]

Furthermore, the general EU consumer policy (Arts. 12, 114 and 169 TFEU) also has a direct influence on cloud computing, since its main goal is the promotion of consumers' safety and economic interests, as well as the right to information to protect their interests. Although legislative responsibility in this area is shared between the European Union and EU Member States, it was mainly the EU who took measures to approximate EU countries' consumer legislation; however, EU Member States were free to keep or introduce stricter consumer protection measures than those laid down by the EU, as long as they are compatible with the Treaty and the Commission is notified of them. These general guidelines will also apply to Cloud Computing in the scope of the E-Commerce Directive and, potentially, the Digital Content Directive.

3.2 Secondary sources

In this chapter, I will also analyse the main secondary legislative acts produced by the EU, which have a direct influence on cloud computing. I will briefly address the Data Protection Directive[61] (**DPD**) for historical reasons, and then will focus on the GDPR, which is applicable as of May 2018 and replaced the DPD. I will further assess the ePrivacy Directive[62] (and the proposal for ePrivacy Regulation Proposal), the NIS Directive[63], and the E-Commerce Directive[64],

[58] Following the amendment introduced in 1999, the EU became a party to the Convention for the protection of individuals with regard to the automatic processing of personal data, or Convention 108, as it is commonly referred. The Convention applies to all data processing carried out by both the private and public sector and envisages to protect individuals against abuses following the collection and processing of personal data, furthermore, it established the right of individuals to information regarding the data stored about them.

[59] Currently, Uruguay is the only non-member of the Council of Europe which has ratified the Convention.

[60] As indicated in the "Handbook on European data protection law", of European Union Agency for Fundamental Rights and the Council of Europe, 2018, p.26.

[61] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[62] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[63] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1, 19.7.2016.

[64] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16

the Consumer Rights Directive (CRD)[65] and the DCD, which provide specific obligations towards CSPs.

3.2.1 General Data Protection Regulation (GDPR)

3.2.1.1 Historical background

The GDPR was published on 2016 and has been applicable since 25 May 2018, replacing the DPD. This regulation attracted much attention and is the result of significant lobbying to increase harmonisation across the EU on personal data, which has been achieved in most areas.[66]

As such, and even though it has been repealed, it should be noted that the DPD was considered the cornerstone of the European legislation on data protection, aiming to ensure that the fundamental rights of data subjects were duly safeguarded, while guaranteeing that personal data could flow freely between the Member States. The DPD intended to strike a balance between the necessity of ensuring the privacy of individuals and the development of the European internal market and the promotion of the interests of commercial entities in the EU zone. Also, given the scope of EU primary law in force at the time of the adoption of the DPD, the material scope of the Directive did not encompass matters of police and criminal justice cooperation.[67]

Additionally, the DPD established the A29WP, comprised by the national EU data protection regulators and the European Data Supervisor and whose main objectives included the assessment of: (i) the uniform application of the DPD on all Member States; (ii) the level of protection granted by third countries; (iii) proposed amendments to the DPD and of additional measures to safeguard the right and freedoms of natural persons, and; (iv) the codes of conduct adopted at EU level. A29WP had a significant relevance as an advisory body, however, the materials it produced (opinions, working documents, etc.) did not reflect the position of the European Commission, nor were they binding on EU Member States' courts or the CJEU. In this sense,

[65] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, revised by Directive (EU)2015/2302 of the European Parliament and of the Council of 25 November 2015 and Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019.

[66] Such harmonisation does not include personal data on the fields of journalism and freedom of speech (Art. 85) and employment law (Art. 88), or that outside EU's scope, e.g. national security (Art. 2(2)(a) and Rec. 16).

[67] Data protection in these matters was mainly established by Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350. However, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, has been published in April 2016 and obliges Member States to transpose it by May 8, 2018.

it should be highlighted that, under the DPD, A29WP clarified the concepts of personal data and data subject, as well that of controller and processor. Under the GDPR, this mechanism has been replaced by the EDPB and its powers have been expanded.

3.2.1.2 Material and Territorial Scope

As defined in its Art. 2[68], the GDPR applies to any processing[69] of personal data by automatic means or by other means forming part of a filling system; its scope specifically excludes activities: (i) falling outside of the scope of EU law, (ii) of Member States relating to common foreign and security policy, (iii) usages by natural persons for household purposes[70] and by competent authorities for purposes of detecting and prosecuting criminal offences.

Concerning its territorial scope (Art. 3), the GDPR will apply to: (i) any processing of personal data in the context of the activities of an establishment of an entity in the EU, regardless of whether the processing takes place in the EU or not (Rec.22), as well as to any processing activities pertaining to (ii) the offering of good or services to data subjects in the EU (Rec.23) or to (iii) the monitoring of their behaviour within the EU (Rec.24), even if such controller or processor are not established in the EU[71]; hence, non-EU companies targeting EU data subjects[72] are now under the scope of the GDPR.[73] It is further worth highlighting that the GDPR provided much needed clarity and precision on this matter, which under the DPD was subject to substantial considerations by scholars[74] and policy-makers[75].

---

[68] "This Regulation applies to the processing of personal data wholly or partly by automatic means and to the processing other than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."

[69] The broad concept of processing as defined in Art. 4(2) implies that most uses involving personal data will fall under the GDPR, insofar as covered by its material and territorial scope.

[70] Rec. 18 has further clarified that such exclusion applies to social networking and online activity in the context of household activities, which points to a departure from CJEU case law on the matter (e.g. Case C-101/2001). On this matter see also, van Alsenoy, Brendan, "The Evolving Role of the Individual Under EU Data Protection Law", CiTiP Working Paper 23/2015, 2015, and Rudgard, Sian, "Origins and Historical Context of Data Protection Law", in European Data Protection: Law and Practice, ed. Ustaran, Eduardo, IAPP, 2018, pp. 97-98.

[71] The GDPR will also apply where Member State law applies by virtue of public international law (Art 3 (3)).

[72] See Art. 3(2). Rec. 23 clarifies that such offering should be more than mere access, but that factors such as use of language or currency generally used in Member State or mention to consumers/users in the EU may make clear that the controller intends to offer goods/services to data subjects in EU. Rec. 24 also provides guidance concerning the concept of monitoring of behaviour.

[73] For further information, see "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)", European Data Protection Board, 2018.

[74] See Hon, Kuan W., Hörnle, Julia and Millard, Christopher, "Which Law(s) Apply to Personal Data in Clouds", in Cloud Computing Law, ed. Millard, Christopher, Oxford University Press, 2013, pp. 220 – 248. See also Moerel, Lokke, "The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?," International Data Privacy Law 1, no. 1,2011, pp. 28–46.

[75] See A29WP's Opinion 8/2010 on applicable law, WP 179, 2010 (and WP 179 update, 2015), and the "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites", WP 56, 2002.

Concerning point (i) above, it should be noted that several CJEU rulings[76] have confirmed the broad interpretation of such notion, which is considered verified if an entity exercises effective and real activity – even a minimal one – through stable arrangements.[77] Also, the CJEU has clarified on the concept of "in the context of the activities of an establishment", indicating that a sufficient connection is deemed to exist if the activities of an EU entity "are inextricably linked" to the processing activities undertaken by a non-EU entity.[78]

3.2.1.3 Main concepts of the GDPR

3.2.1.3.1 Personal Data and Data Subject

The definition of personal data is vital to any consideration of the impacts of the GDPR on cloud computing services, given that data not considered as such may be processed, by any means, free of the requirements imposed by data protection law within a cloud. In order to fully understand whether cloud computing services fall into the scope of GDPR, the concept of personal data and data subject should be clarified.

The GDPR defines, in Art. 4(a) personal data as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factor specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person"

As such, regardless of its nature or context, personal data will comprise four elements:

1. "any information" – any type of statements concerning an individual, covering both objective (e.g., the presence of substances in one's blood) and subjective information (e.g. opinions or comments); this concept encompasses information kept in any format (alphabetical, numerical, graphical, photographic or acoustic) and in any support (e.g. paper, computer memory or videotape).

[76] See in particular judgement of 13 May 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317; judgement of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639 ; judgement of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388; and, judgement of 28 July 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612.

[77] See *Weltimmo*, para 29 and 31; in any case, this notion has nonetheless limits as explained in *Verein für Konsumenteninformation*, para 76.

[78] See *Google Spain*, para 56; such interpretation was subject to comments by A29WP in its update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain (WP179update), 2015 (in particular, pp.4-6) and, more recently, by the EDPB see note 73 (in particular, pp.7-8).

2. "relating to" – relates to information on an individual, but also information indirectly about individuals, resulting from ownership or possession of an object by an individual. A29WP indicated that such information should present an element of "content", "purpose" or "result" to be considered personal data[79]; thus, such element is to be interpreted subjectively[80].

3. "identified or identifiable" – a person is identified or identifiable when they can be distinguished or passible of so from others, respectively. Fragments of information (i.e. "identifiers") hold a privileged and close connection with an individual and can provide direct or indirect identifiers[81]; considering the technological evolution, such indirect identification is considerably easier to achieve and special attention should be allotted to it.[82]

   Another relevant issue, at this point, is pseudonymised data and anonymised data[83]; while the first consists in the disguising of identities through the use of pseudonyms, the latter pertains to the process of removal of data relating to a natural person, which can then no longer be identified, whether by the data controller or by any other person. However, these systems will only preclude the application of GDPR, when the data available no longer enables the identification of the individual.[84]

4. "natural person" – the Regulation applies to any natural person, regardless of their nationality or residency,[85] while not extending to personal data of deceased persons;[86] however, caution should be used when disclosing this type of data.[87]

---

[79] See A29WP's Opinion 4/2007 on the concept of personal data, WP136, 2007, pp. 9-12.
[80] See judgment of 24 November 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, paragraph 51 .
[81] Indirect identification is limited to "all of the means likely reasonably to be used either by the controller or by any other person to identify the said person" (Rec. 26 GDPR). In this regard, CJEU has further clarified the concept, that indirect identifiers (in this case, dynamic IP addresses) may be considered personal data if the possibility (even if remote) to identify the data subject persists, see judgment of 19 October 2016, Breyer, C‑582/14, U:C:2016:779, paragraphs 45 to 49.
[82] [82] See Art. 4 (1). Additional compliance may result from the use of cookies containing information on location data, online identifiers or genetic data, which may then fall under the definition of personal data.
[83] For different methods of anonymising or pseudonymising data, see Hon, K., Bradshaw, S., Millard, C. and Walden, I., *The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing*, in International Data Privacy Law, Vol. I, No. 4, , 2011, pp 214 – 222, as well as Opinion 05/2014 on Anonymisation Techniques, WP 216, 2014.
[84] Such analysis has to be conducted on a case by case basis and taking into account "all of the means likely reasonably to be used either by the controller or by any other person to identify the said person" (Rec. 26 GDPR).
[85] See recital 2.
[86] Recital 27 clarifies this matter, while indicating that Member states may also legislate on the matter.
[87] From a corporate standpoint, it will probably be less burdensome for controllers to maintain the same level of protection for living and deceased data subjects, than to create two separate sets of data, especially since controllers may not dispose of manners to monitor accurately such information. Also, we note that some national legislation may extend the scope of these rules, when the legislator decides that a legitimate interest may exist to justify it, as the

From points 3 and 4. above, we can further extract the definition of data subject as any "identified or identifiable natural person".

3.2.1.3.2 Sensitive Personal Data

In addition, the GDPR identifies special categories of data[88], given that their processing may create significant risks to individuals' fundamental rights and freedoms, hence, warranting special protection. Special attention should be drawn, regarding biometric data, since it can be considered as information on one individual, but also as a link between specific information and the individual[89], which may allow his/her identification; this type of data is particularly sensitive and specific rules of the GDPR apply[90]. Such broad interpretation of sensitive data has been confirmed by the CJEU in Lindqvist[91] and is further aligned with the jurisprudence of the European Court of Human Rights ('ECtHR)[92], as well as with the rules CFREU[93].

Should data be classified as sensitive data, Art. 9 (1) GDPR establishes a general principle prohibiting its processing; however, exceptions to such principle are set forth in its Art. 9 (2), which include explicit consent, performance of specific obligations or rights in the field of employment law, vital interests of the data subject, legitimate interests of others and public interest.. Lastly, Member States may introduce further conditions or limitation regarding the processing of genetic, biometric or health data.

3.2.1.3.3 Controllers and Processors

A good understanding of the scope of the GDPR requires also the analysis of the concepts of controller and processor[94], which are crucial in the allocation of responsibility within the cloud

---

CJEU has indicated in *Lindqvist* (judgement of 6 November 2003, *Lindqvist*, C‑101/01, EU:C:2003:596, paragraph 43); see also A29WP's "Opinion 4/2007 on the concept of personal data", WP136, 2007, and op. cit in note 83, pp 213-214.

[88] As per Art. 9 (1) as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

[89] A29WP, in Opinion 4/2007, presented the example of fingertips and DNA, which provide a unique identifier.

[90] However, special rules may also apply to the collection, storage and use of tissue samples. For more information, see Council of Europe Recommendation No. (2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin, of 15.3.2006.

[91] See judgement of 6 November 2003, *Lindqvist*, C‑101/01, EU:C:2003:596, paragraph 24.

[92] Judgement of the ECHR in Amann v Switzerland of 16.2.2000, para68-70.

[93] See Art. 8 CFREU.

[94] Hon, Kuan W., Millard, Christopher, and Walden, Ian, *Who is responsible for 'personal data' in cloud computing? – The cloud of unknowing, Part 2*, in International Data Privacy Law, Vol. 2, No. 1, 2012.

computing relation. The concept of controller was firstly codified in 1981;[95] however, the concept currently established in the GDPR is more comprehensive, defining it as *"the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data"*.[96]

As per the definition above, the controller will have the power and the legal duty to determine the purposes and means of the data processing, which determine who is the *de facto* controller of data and provide for (and limit) the possible scope of action of the processor..[97] Also, considering the complexity of cloud computing, there may be situations where more than one CSP will fit the definition of controller,[98] which might lead to difficulties when determining responsibility. On this subject, A29WP clarified that the joint determination does not need to be equally shared, but that the involved parties may distribute and determine the responsibilities and obligations amongst themselves at their own discretion; however, overall compliance with the data protection obligations have to be assured. [99]

In addition, the processing has to be consistent with the data subject rights[100] and must not be transferred outside of the Europe Economic Area ("EEA"), except when the country to which it is transferred ensures an adequate level of protection for the rights and freedoms of data subjects.[101]

On the other hand, if a controller decides to use another entity to process personal data, it must select a processor providing 'sufficient guarantees' to implement appropriate technical and organisational security of such data and must ensure that such relation is governed by a contract or other legal act that is binding on the processor.[102]

Accordingly, a data processor is defined as the "*natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*"[103]. Hence, two major requirements

---

[95] See Art. 2 (d) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[96] Art. 4(7).
[97] As per A29WP's "Opinion 1/2010 on the concepts of "controller" and "processor"", WP169, 2010, p. 16, the "[d]etermination of the "means" therefore includes both technical and organizational questions where the decision can be well delegated to processors (as e.g. "which hardware or software shall be used?") and essential elements which are traditionally and inherently reserved to the determination of the controller, such as "which data shall be processed?", "for how long shall they be processed?", "who shall have access to them?", and so on".
[98] The definition clearly allows for the existence of more than one controller, regarding the same personal data. Despite this, some Member States (for instance, France and Poland) neither explicitly recognize such possibility, nor provide for the concept of co-controller.
[99] See A29WP's Opinion 1/2010 (WP 169), p. 19.
[100] Art. 12 to 23; especially relevant to CSPs will be the right to be forgotten (Art. 17 and Rec. 65 and 66) and the right to data portability (Art. 13 (2)(b) and 20 and Rec. 68)..
[101] See Chapter V of the GDPR.
[102] See Art. 28 (3); such contract or legal act shall include, at least, the items indicated in Article 28 (3).
[103] Art.4(8)

are needed for an entity to be qualified as a data processor: firstly, the processor must be a separate legal entity from the controller and, secondly, it must process the data on behalf of the controller.

One significant change of the GDPR in relation to the DPD is that processors will be directly subject to the GDPR's obligations; such derives from the minimum stipulations to be included in the controller-processor agreement, but also from other obligations emerging directly from the GDPR, including the maintenance of a written record of processing activities (Art. 30 (2) and Rec. 82), the designation of a Data Protection Officer (Art. 37) and the need to notify the controller in the event of a personal data breach (Art. 33 (2).); additionally, the processor has a duty to immediately inform the controller if it considers that an instruction infringes the applicable data protection obligations (Art. 28 (3), last sentence). Lastly, it is worth noting that any obligations imposed on the processor by the controller shall be imposed on further sub-processors, even though the controller may restrict the use of sub-processors to guarantee the security of personal data.[104]

Consequently, it is important to consider which (if any) of the parties involved in a cloud computing relation are controllers, processors – or neither, as some authors state[105] –, as well as to highlight that the same entity may act as controller in processing activities of certain personal data and as a processor for others, a demonstration that cloud computing is "blurring the distinction between data controllers, processors and data subjects".[106]

3.2.1.3.4 GDPR Principles and Obligations

Under Art. 5 GDPR, the controller has the responsibility of ensuring that any processing of personal data complies with the following principles:

a) Principles of lawfulness, fairness and transparency – personal data can only be processed if a legal ground for such exists (Art. 6)[107] and data subjects shall be informed

[104] See Art.28(2); A29WP's Opinion 1/2010 stated that "the obligations and responsibilities stemming from data protection legislation should be clearly allocated and not dispersed along the chain of outsourcing/subcontracting. In other words, one should avoid a chain of (sub-) processors that would dilute or even prevent effective control and clear responsibility for processing activities, unless the responsibilities of the various parties in the chain are clearly established."

[105] See Hon et al., op. cit in note 94, pp. 3-18.

[106] See A29WP's "Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", WP 168, 2009.

[107] This principle should be read in line with the concept of and the conditions for "lawful limitations", under both Art. 52 EUCFR and the jurisprudence of the both the ECtHR and the CJEU. For more information please refer to note 60, pp 42-52.

that their personal data is being processed and the conditions associated to such processing activities, in a concise and clear manner.[108]

b) Principle of purpose limitation – data must be collected for specific, explicit and legitimate purposes and not be processed for further purposes;[109]

c) Principle of data minimisation – the collection and use of personal shall be limited to what is relevant and proportional for achieving the processing purpose(s);[110]

d) Principle of data accuracy – controllers shall implement reasonable measures to ensure that data is accurate and kept up to date; the collected data shall hence only be that which is necessary and proportional to achieve the goal of the purpose.[111]

e) Principle of storage limitation – data shall be kept in a format that allows the identification of data subject for no longer than necessary;[112]

f) Principle of Integrity and Confidentiality – data shall be processed in a secure manner, ensuring its confidentiality and integrity (as well as availability and resilience[113]).

g) Principle of accountability – controllers shall be responsible for the implementing the aforementioned principles and to demonstrate compliance to them[114].

In addition to the aforementioned principles, the GDPR has established the following possible legal basis to process personal data:

1. Consent of the data subject – as per Art. 4(11) consent amounts to a clear affirmative action/statement (as per Rec. 32, "silence, pre-ticked boxes or inactivity should not therefore constitute consent"), freely given (Rec.43), specific, informed (Rec.42) and unambiguous; as per Art. 7, consent shall be presented in an intelligible and easily accessible form, using clear and plain language, in a manner that is distinguishable from others matters and it shall be as easy to withdraw consent as it was to give it (Art. 7(3)). Before relying on consent, controllers should consider that conditions for con-

[108] See Arts. 12-14.
[109] However, further processing can be allowed if considered compatible with the initial purpose – for more information see Rec. 50.
[110] Nowadays, this principle also includes a supplementary aspect, inviting controllers to use privacy-enhancing techniques, such as anonymization to decrease risks inherent to extensive processing systems, For more data on the concept of necessity and proportionality regarding processing of personal data, please see A29WP Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP211), 2014, and the EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019.
[111] See Rec. 39.
[112] See Rec. 39; these periods should be limited to the strict minimum time necessary and controller should verify statutory data retention periods in relation to certain types of data (e.g. employment data).
[113] Art.31(1) (b).
[114] See Art. 5(2). For more information, please see A29WP's Opinion 3/2010 on the principle of accountability (WP 173), 2010 and Art 14 of the OECD's Guidelines on governing the Protection of Privacy and transborder flows of personal data, 2013.

sent may be inappropriate for certain activities[115] and that additional conditions will apply when relying on such legal basis (e.g. see Arts. 7(3) and Art. 20).[116]

2. Performance of a contract – processing is necessary to perform a contract or to take steps required by data subject prior to entering into a contract;[117]

3. Public interest or exercise of official authority – as per Rec. 45, such processing shall be based in EU or Member State law, which shall in any case "meet an objective of public interest and be proportionate to the legitimate aim pursued" (Art. 6 (3); in this context, the CJEU indicated that such concept "has its own independent meaning in Community law and (…) must be interpreted in a manner which fully reflects the objective of the directive", namely recalling that Member State may only impose limitations on citizens (which are likely to involve processing of personal data) to the extent those are necessary to achieve a particular purpose;[118]

4. Compliance with controller's legal obligation – as per Rec. 45, such processing shall be based in EU or Member State law, within the limits indicated in 3. above;

5. Vital interests of the data subject – when processing relates to the wellbeing/survival of the data subject (Rec. 112);

6. Legitimate interests of the controller – this concept relies on a "balancing test", between the legitimate interests of the controller (e.g. commercial interests) and fundamental rights and freedoms of the data subject.[119]

   Note: As indicated above, the processing of special categories of personal data is subject to more stringent legal bases, as set forth in Art. 9(2).

In addition to the obligations above, controllers shall implement appropriate measures to ensure the following data subjects' rights and their effective exercise:[120]

---

[115] For instance, consent in the context of an employment relation will hardly be perceived as freely given, due to the significant imbalance between the parties (Rec. 43).
[116] The concept of consent and concepts related to it (such as control, transparency, activity/timing) have been thoroughly assessed by A29WP', in "Opinion 15/2011 on the definition of consent", WP 187, 2011; an update on this has been recently issued by the EDPB in its "Guidelines 05/2020on consent under Regulation 2016/67", 2020.
[117] For more detail, please see the EDPB's "Guidelines2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects", 2019,
[118] See judgement of 16 December 2008, *Huber*, C-542/06, ECLI:EU:C:2008:724, paras 52 to 58.
[119] See Rec. 47-19; further details, namely on when this concept and on how to balance it against the rights of data subjects can be found in A29WP's "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", WP217, 2014.
[120] In order to ensure that requests by data subjects on this matter are addressed in a timely manner, the legislator has established that the controller shall reply within one month of the receipt of a request, as per Art. 12(3).

- Right to transparent communication and information (see Arts. 12 to 14),
- Right of access (Art. 15);
- Right to rectification (Art. 16), right to erasure – commonly known as 'right to be forgotten' (Art. 17) – and to restriction of processing (Art.18)[121];
- Right to data portability (Art. 20):
- Right to object to processing (Art. 21) and the right to not be subject to automated decision-making (Art.22).

Controllers shall further carefully consider the limitations on the transfer of personal data to third countries, given the specific relevance of this for cloud computing and considering that data may be transferred to servers in third countries. Art. 1 (3) establishes the principle of free movement of personal within the Union and to countries which are part of EEA, for purposes relating to the internal market.

Such general freedom may be further extended to third countries (or a territory or one or more specified sectors within that third country) if those are deemed to ensure an adequate level of protection, following the assessment of the European Commission (Art 45 (3)); such adequacy decision shall be subject to ongoing monitoring.

Nonetheless, even if the Commission considers that an adequate level of protection is not ensured, transfers of personal of data to third countries may still occur if the recipient has established adequate data protection safeguards, which may include any of the following:

- Binding corporate rules (BCRs) – these rules allow the transfer to personal data between several entities of a specific corporate group internationally, if such agreement fulfils the conditions indicated in Art. 47 (e.g. being legally binding, applying the data protection principles and safeguarding data subjects' rights);[122]
- Standard Contractual Clauses (SCC) – are clauses adopted in accordance to Art. 93 (2) GDPR which offer sufficient safeguards to personal data aimed to be transferred internationally; controllers may also include these clauses in their own contracts or to

[121] In conjugation with these rights, the controller shall also communicate any rectification or erasure of data to the relevant data subject, under certain conditions (see Art. 19).

[122] BCRs are considered the gold standard of global data protection, since they implement a global framework based on European privacy standards. For further details see the following A29WP documents: "Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data", WP 133, 2007, "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", WP 153, 2008, "Working Document setting up a framework for the structure of Binding Corporate Rules" WP154, 2008, and "Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities". WP195a, 2012; see also Pothos, Mary, "Accountability Requirements", in European Data Protection: Law and Practice, ed. Ustaran, Eduardo, IAPP, 2018, pp. 209-210.

add further clauses or safeguards, insofar as such does not contradict the Commission approved ones;[123] the question whether the SCCs offer the level of protection when personal data is transferred to the US under this mechanism is currently pending before the CJEU;[124]

- Codes of conduct (Art. 40) and certification mechanisms (Art. 42) – both are self-regulation mechanisms aimed at demonstrating compliance with the GDPR (Art. 40 (1) and 42(1) GDPR), subject to monitoring/certification by external independent entities;
- Special international agreements.[125]

Lastly, one should also consider the EU-US Privacy Shield,[126] which was adopted by the Commission on 12th July 2016 and that substituted the previous US Safe Harbour Decision,[127] which was deemed invalid by the CJEU, in its judgment in Schrems.[128] The Privacy Shield aims to protect the fundamental rights of EU citizens whose personal data are transferred to the United States (US) and to ensure legal clarity for businesses relying on transatlantic data transfers. Also, it was intended to reflect the concerns and requirements put forth in Schrems and to provide for stricter obligations on US organisations, by requiring the US to monitor and enforce them more robustly in cooperation with the relevant European Data Protection Authority (DPA). The Privacy Shield is based on a system of self-certification by which US organisations envisaging to process personal data from EU data subjects commit to the following Privacy Principles:

---

[123] Currently there are three sets of standard contractual clauses, regarding the following models: the controller to controller SCC (Commission Decision 2001/497/EC:), the alternative controller to controller SCC (Commission Decision 2004/915/EC) and the controller to processor SCC (Commission Decision 2010/87/EU). For further details, see A29WP "Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" considered as compliant with the EC Model Clauses", WP226, 2014.

[124] See Case C-311/18, Data Protection Commissioner and Facebook Ireland, Maximilian Schrems ("Schrems II"), pending judgement; the opinion of AG Saugmandsgaard Øe on this reaffirms the sufficiency of the mechanism itself, while recalling the controller's obligation to "suspend or prohibit that a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with." (para. 128). Additionally, it is likely that this case and the CJEU's judgement will likely have a further impact on the Privacy Shield , as part of the context to the issues raised.

[125] E.g. the Passenger Name Records (PNR) and the SWIFT (Society for Worldwide Interbank Financial Telecommunication). For more information see Moerel, Lokke, "Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers", Oxford University Press, 2012.

[126] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield

[127] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

[128] Judgment of 6 October 2015, Schrems, C-362/14, ECLI:EU:C:2015:650. See also, CJEU's Press Release No 117/15, 2015.

- **Notice principle** – provision of information on key elements when processing personal data, such as type of data, purpose of processing, right of access, conditions for onward transfer and liability;

- **Choice principle** – data subjects may elect not to have their personal data disclosed to a third party or used for "materially different" purposes – opt out; in case of sensitive data, express consent must be given – opt in;

- **Security principle** – organisations shall create, maintain, use and disseminate personal data under "reasonable and appropriate" security measures, considering the risk of processing operations;

- **Data integrity and purpose limitation principle** – collection of personal data shall be limited to what is relevant and required, and not be used for purposes incompatible with that for which it was originally collected;

- **Access principle** – data subjects have a right to obtain from an organisation a confirmation if it is processing personal data relating to them;

- **Accountability for onward transfer principle** – onward transfers can only take place, for (i) limited and specified purposes, (ii) on the basis of a contract and (iii) only if that contract ensures the same level of protection as the Privacy Principles;

- **Recourse, enforcement and liability principle** – organisations must set up robust mechanisms to ensure compliance with the Privacy Principles, by annually recertifying, and shall verify that their own privacy policies comply with the Privacy Principles, either through a system of self-assessment or by external compliance reviews.

In this context, the new EU-U.S. Privacy Shield has had a significate impact on commercial activities, contributing to an increase in transparency. Also, to further ensure organisations' compliance, it provides new and better oversight mechanisms, it enforces sanctions and/or exclusions for non-compliant organisations and includes stricter conditions for onward transfers. On the other hand, concerning by the US Government, it aims to improve safeguards and transparency obligations, namely by imposing limitations, safeguards and oversight procedures on access to personal data by authorities, preventing (partially) indiscriminate or mass surveillance by U.S. authorities, and introducing a "Privacy Shield Ombudsperson" – independent from the intelligence community, who shall guarantee investigation of individual complaints and provide

individuals information if US laws were observed or, in case they were not, information that such noncompliance has been remedied.

Furthermore, the Privacy Shield introduces several redress possibilities, either (i) directly with the organisation, or (ii) via an Alternative Dispute Resolution mechanism, or (iii) by presenting a complaint to a local DPA which will liaise with the US Department of Commerce (DoC)/Federal Trade Commission (FTC) to ensure that unresolved complaints by EU citizens are investigated and solved, or ultimately (iv) via the Privacy Shield Panel, which is a last resort arbitration possibility aiming to achieve an enforceable decision. However, A29WP[129] and various sectors of public society expressed their dissatisfaction towards such Decision.[130]

The Shield also provides for an Annual Joint Review to monitor its application and functioning, which will include information on access to data by law enforcement and for national security purposes. The first review confirmed that the Privacy Shield provided an adequate level of protection, while including ten recommendations to improve its functioning.[131] The second report maintained such adequacy findings, while highlighting some concerns and encouraging the US "to adopt a comprehensive system of privacy and data protection and to become a Party to the Council of Europe's Convention 108", in order to ensure convergence between the two systems in the longer term.[132] The third annual review has once again confirmed the previous adequacy finds;[133] however, its accompanying working document, has highlighted the need to "clarify certain aspects of the [US] legal framework, the functioning of different oversight mechanisms and the possibilities for redress,"[134] in light of the litigation on the matter pending before the CJEU.[135]

---

[129] A29WP raised concerns on the fact that the Decision neither obliged organisations to delete data no longer necessary, nor excluded the continued collection of massive and indiscriminate data; additionally, it had doubts that the Ombudsperson had sufficient powers to function effectively and recommended the introduction of a glossary of key data protection notions to ensure correct definition and consistent application; see A29WP's Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP 238, 2016.

[130] See European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP)); 'U.S. Must Reassure EU on Privacy Protections, Official Says'. 30/03/17, Bloomberg, (www.bna.com/us-reassure-eu-n57982085959) and 'Privacy Shield Will Not Survive Legal Challenge, Says Schrems', 13/07/16, EUObservser, (www.euobserver.com/digital/134322).

[131] Report from the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU-U.S. Privacy Shield, COM (2017) 611 final, 2017, pp. 4-7.

[132] Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, COM (2018) 860 final, 2018.

[133] Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield, COM (2019) 495 final, 2019.

[134] Staff Working Document. accompanying the Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield, SWD (2019) 390 final, 2019.

[135] In Case T-738/16, La Quadrature du Net v. Commission, pending judgement, the applicants are seeking to invalidate the Privacy Shield, on the basis that it contains insufficient protections against US Government access to personal data transferred from the EU; the hearing of this case has been vacated to await the judgment of the CJEU in Schrems II.

In the absence of an adequacy decision or of appropriate safeguards into place, the transfer of personal data to third countries may still be allowed under the circumstances indicated in Art. 49(1), which are more stringent than those included in Arts 6 and 9.

Lastly, if a transfer of personal data cannot be framed in any of the scenarios/conditions indicated above, it can nonetheless still take place insofar as (i) it is not repetitive, (ii) concerns a limited number of data subjects, (iii) is necessary for the purposes of a compelling legitimate interest of the controller (and not overriding the rights and freedoms of data subjects) and (iv) the controller, considering the circumstances of such transfer and the data in case, has implemented adequate safeguards to protect such data. Should all of these conditions be fulfilled, the controller may transfer such data, while in parallel it shall inform the relevant DPA of such transfer and fulfilling its information obligations (see Arts. 13 and 14 GDPR) towards the data subjects, especially on the compelling legitimate interests which motivated the transfer.

V. Considering the above, we conclude that the application of the controller and processor concepts to cloud computing is far from straightforward, given the complexity of structures and the potential variety of services to be provided by a CSP.

This approach can become even more complex if one adopts the perspective that certain CSPs just provide for "facilities",[136] ultimately putting into question whether such CSP would even fall into the concepts of processor and/or controller.[137] In this sense, it should be noted that there is still a certain degree of legal uncertainty regarding the applicability of the GDPR to encrypted data, despite some authors defending that a CSP who processes encrypted data will not be processing personal data, insofar as it cannot access that data even in the event of a breach of its servers.[138]

---

[136] For example, an IaaS provider may rely on the notion that it is only providing a (virtual) structure, without being aware of that personal data is included in their systems, , or being able to access such data; in that sense, their services could be considered only as tools/conduits to be used by the controllers/processors.

[137] Cf. supra note 94, p. 14 et seq; particularly, p.19,: "[I]t is arguable that certain infrastructure providers are not even 'processors', particularly where they are used only for processing power. It is more difficult to do so where the service provided consists of or includes persistent storage of data (…). However, the provider will often not know the nature of data stored with it, so it seems problematic that its status should depend on what data its customer decides to store and how well the customer encrypts or anonymises the data". These authors further consider that CSPs should be considered mere neutral intermediaries, as per the meaning (and liability regime) of the E-Commerce Directive.

[138] See Spindler, Gerald and Schmechel, Philipp, "Personal Data and Encryption in the European General Data Protection Regulation", 7 JIPITEC, 163, 2016, paras 79-81; see also, Finck, Michèle, and Pallas, Frank, "They Who Must Not Be Identified-Distinguishing Personal from Non-Personal Data Under the GDPR," Max Planck Institute for Innovation & Competition Research Paper, no. 19–14, 2019.

Considering the typical service structures in cloud computing, the CSP will mainly act as a processor of personal data, in which case processing shall take place under a written agreement with the controller and a CSP shall further follow the processing instructions of a controller; nonetheless, the processor shall immediately inform the controller, if it believes that the controller's instructions are contrary to the GDPR or to other EU or Member State laws. Lastly, CSP shall avoid performing personal data processing activities outside the scope of the contract it has with the controller, as it shall be considered a controller for such activity and be subject to the full compliance obligations of a controller in relation to that processing (Art. 28(10) GDPR)

In most cases, a CSP will in parallel to its activities as a processor, be collecting and processing personal data as a controller, due to its agreement with the processor (e.g. processing of contact details of the processor's staff in a CRM database), which shall trigger the application of GDPR to itself as a controller for such specific personal data.

Considering the explanation of the relevant concepts above, we confirm that data protection will, in any instance, be a relevant legal issue when either availing from a CSP and for the CSP itself, regardless of its classification as controller or processor. Also, it should be highlighted that under the GDPR, the typical complex supply-chains no longer hinder the exercise of data subject rights, even if such data subject cannot recognise if the entity with whom it interacts is the controller, processor or further sub-processors; hence, CSPs shall ensure the implementation of the relevant mechanisms to ensure compliance towards the GDPR.

3.2.2 ePrivacy Directive

The EU Directive 2002/58 on Privacy and Electronic Communications[139] (better known as "ePrivacy" or misleadingly as the "Cookie Directive"), sets out a number of obligations regarding data protection and privacy in electronic communications, including confidentiality of information, treatment of traffic data, spam and cookies. Thus, the ePrivacy Directive will be applicable if a CSP acts as a provider of electronic communication services. Thus, under this framework, CSPs will be required to ensure compliance with obligations regarding secrecy of communications and personal data protection.

The Directive further dictates that the storing of information or gaining access to information stored (not limited to personal data) in the "terminal equipment" of a user to trace its

[139] See note 62.

activities (e.g. cookies)[140] can only occur, if the user has given consent and was provided with the relevant information, namely regarding the purposes of such processing. As a general rule, CSPs will have to comply with the main provisions concerning the prohibition of unsolicited e-mail and other messages for marketing purposes and the opt-in regime, meaning that users have to provide consent for cookies which are not "strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user"[141]. Nonetheless, the preamble of the Directive denotes the legitimacy of using cookies either for "analysing the effectiveness of a website design and advertising, and in verifying the identity of users engaged in on-line transactions", but recalls that users should be "provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using" and that such users should also be given the "opportunity to refuse to have a cookie or similar device stored on their terminal".[142] This is further confirmed by Art. 5 (3) of the amended version of the ePrivacy Directive.

Art. 4 of this Directive reaffirms the need of a provider to take appropriate technical and organisational measures to safeguard the security of its services, namely to ensure that personal data can be accessed only by authorised personnel and for legally authorised purposes and that such measure shall be able to be audited by the relevant national authorities.[143] Also, in case of a personal data breach, the provider "shall, without undue delay, notify the personal data breach to the competent national authority" and that if such breach "is likely to adversely affect the personal data or privacy of a subscriber or individual", the provider shall additionally notify the subscriber or individual, unless it can demonstrate to the competent authority that it has implemented adequate technological protection measures, which render the data unintelligible to persons not authorised to access it.[144] By means of the transpositions of the Directive by State Members, these provisions have a direct impact on cloud service providers and the contract with their clients and, thus, should be closely observed by them. Additionally, CSPs which fall under the scope of the Directive will also have to "ensure the confidentiality of communications and related traffic data".

---

[140] For further information on "cookies" and their use, please refer to Lanois, Paul, "Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?", Northwestern Journal of Technology and Intellectual Property, Volume 9, 2010.

[141] Rec. 66 of Directive 2009/136.

[142] Rec. 25 of Directive 2002/58.

[143] Art. 4 (1) and (1a) of Directive 2002/58, as amended by Directive 2009/136.

[144] Art. 4 (3) of the Directive 2002/58, as amended by Directive 2009/136. Art. 4 further determines which data is to be provided to the national authority and to the subscriber and individual.

3.2.2.1 Proposal for an ePrivacy Regulation

An ePrivacy Regulation Proposal[145] has been presented in January 2017, which was intended to be "*lex specialis* to the GDPR" and to "particularise and complement it as regards electronic communications data that qualify as personal data".[146]

In this context, we note that the Commission proposed ePrivacy Regulation broadens the scope of the Directive, encompassing new forms of electronic communications, such as Over The Top (OTT) providers – i.e. providers of messaging apps, Voice over IP (VOIP) services, e-mail platforms and similar services –, as well as Internet of Things (IoT) and Machine-to-Machine (M2M) communications, in addition, to anyone using cookies or similar tracking technologies (like fingerprinting).[147] Also, much like the GDPR, the proposed Regulation will apply to entities anywhere in the globe providing publicly available electronic communications services to users in the EU or gathering data from the devices of those users.[148]

Additionally, the proposed regulation introduces new rules concerning communications' content and metadata – replacing the term "traffic data" –, which allow for apparent wider uses than the current Directive.[149] The proposed regulation still maintains the consent requirement for cookies, with the exception of first party cookies for analytics, and will likely end the typical cookie banners, since, instead of having browsers blocking all cookies by default, it intends to have browsers and similar software providing users with cookies and tracking controls.[150]

In line with the GDPR, the proposal also establishes significant fines for breaches with administrative fines up to 20.000.000 EUR or up to 4% of annual worldwide turnover.[151]

Originally, the Commission aimed to have the new ePrivacy Regulation enter into force on the same date as the GDPR.[152] Nonetheless, bearing in mind that the diverse drafts proposed have so far have been rejected,[153] it is very likely that the ePrivacy Regulation will not enter into force before 2023.

---

[145] See note 54.
[146] See Explanatory Memorandum, section 1.2, COM (2017) 10 final.
[147] See Art. 2, COM (2017) 10 final.
[148] See Art. 3, COM (2017) 10 final.
[149] See Art. 6, COM (2017) 10 final.
[150] See Explanatory Memorandum, section 3.4 and rec. 22-24, COM (2017) 10 final.
[151] See Art. 23, COM (2017) 10 final.
[152] See Art. 27, COM (2017) 10 final
[153] Since December 2017, the Estonian, Bulgarian, Austrian, Romanian and Finish Council presidencies have published their own drafts, without success. To accompany the evolution of this proposal, refer to: https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform

3.2.3 NIS Directive

The NIS Directive[154] was published on 19th July 2016 and aims to ensure a high common level of network and information security across the EU to prevent security incidents. Considering the increasing number of cyber-attacks, the EU intended to ensure that operators of essential services[155] and Digital Service Providers (DSP)[156] operate in a securitised digital environment throughout EU territory. As in the GDPR, the territorial scope of the NIS Directive is fairly broad, including DSPs which have their main establishment in a Member State, but also those that only offer services within the EU, without having their main establishment there[157]; in the latter case, such DSP will have to designate a representative based in the EU.

Entities such as online marketplaces, search engines and cloud computing services may fall under the scope of the NIS Directive. Accordingly, those entities will have to establish adequate and proportionate technical and organisational security measures,[158] in addition, to being required to report serious incidents to the relevant national authority. Unsurprisingly, it will not be uncommon for CSPs to be subject to both the NIS and the GDPR.[159] Lastly, one should notice that the NIS Directive does not provide for a specific amount of penalties, merely stating that those shall be "effective, proportionate and dissuasive"[160].

In light of the above, the NIS Directive and its corresponding implementing laws will establish a set of new – and eventually comprehensive – obligations on some CSPs, that will probably also entail adjustments to their current procedures and systems. Aside from establishing obligations towards the aforementioned entities, the NIS Directive will also require Member State to implement specific NIS and cybersecurity strategies defining strategies, policies and regulatory measures, as well as to designate national authorities for monitoring its application at national level.

---

[154] See note 63.
[155] The definition of operator of an essential service is indicated in Art. 4 (4) and Art. 5 NIS.
[156] The definition of digital service provider is indicated in Art. 4 (6) and Art. 5 NIS. Please note the existence of a broad exemption of application of the NIS Directive towards micro and small digital enterprises (i.e. which employ fewer than 250 people and have an annual turnover lower than EUR 50 million.
[157] The mere access to a DSP website or services is not sufficient to determine its intention to provide services within the EU; however, the factors pointed as relevant in the GDPR, such as language and currency, as well as indication of EU location of customers/users, may also make apparent that a DSP is offering services in the EU.
[158] See Chapter V NIS, namely Art. 16.
[159] Art. 25 NIS.
[160] Art. 25 NIS.

3.2.4 E-Commerce Directive

The E-Commerce Directive[161] establishes a harmonised set of rules on issues such as the transparency and information requirements for online service providers, which are also applicable to cloud service providers. Furthermore, any entity selling products over the internet – which will almost certainly be the case for CSPs – is required to provide a certain amount of information to users, as well as to ensure that any unsolicited information submitted by it is clearly and unambiguously marked as such.[162] Since other parties offer products and/or services through the cloud provider, the latter will generally only have a partial degree of knowledge about the data they transmit or host, which explains why the allocation of liability follows different rules. These rules determine that intermediaries are exempt from liability arising from third-party content, if the provider did not know of such illegal activity or information or if, upon being aware of such illegality, it acted swiftly to remove or disable access to the illegal information.[163] The Directive further states that providers are not under a general obligation to actively monitor the information or to seek facts or circumstances about illegal activities.[164]

However, the application of the previously mentioned liability limitation to cloud service providers which provide ancillary services (e.g. search engines, platforms with market capabilities, online storage providers) was not clearly established until recently.

In the EU legal framework, the specific regime for liability concerning hyperlinks, remained unclear for a long time. In Joined Cases C-236/08 to C-238/08 (Google France/Inc. v. Louis Vuitton Malletier e.a.), the opinion of the Advocate General (AG) and the CJEU's judgment shed light on this topic. In its decision, the Court, referring to Google, stated that Art. 14 "is to be interpreted as meaning that an internet referencing service constitutes an information society service consisting in the storage of information supplied by the advertiser, with the result that that information is the subject of 'hosting' within the meaning of that article and that the referencing service provider, therefore, cannot be held liable prior to its being informed of the unlawful conduct of that advertiser".[165] Furthermore, the AG in his opinion also indicated that search engines were "already covered by the directive and that the Commission's proposals [referring to Art. 21] are to concern the adaptation of the rules to their specific needs".[166]

---

[161] See note 64.
[162] Art. 5 and 7 E-Commerce Directive.
[163] Art. 12 to 14 E-Commerce Directive.
[164] Art. 15 E-Commerce Directive.
[165] See judgement of 23 March 2010, Google France and Google, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2010:159, para 106
[166] See the Opinion of AG Poiares Maduro of 22 September 2009, Google France and Google, Joined Cases C-236/08 to C-238/08, ECLI:EU:C:2009:569, para. 133

Accordingly, the Court confirmed the application of Art. 14 when "an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored". The Court further confirmed that "If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser's activities, it failed to act expeditiously to remove or to disable access to the data concerned".[167]

The AG also presented arguments that led to a similar conclusion, namely by stating the following: "I construe Art. 15 of that directive not merely as imposing a negative obligation on Member States, but as the very expression of the principle that service providers which seek to benefit from a liability exemption should remain neutral as regards the information they carry or host. (…) This point is best illustrated by comparison with Google's search engine, which is neutral as regards the information it carries". However, when referring to Adwords, it indicated that such neutral position "is not the position as regards the content featured in AdWords. Google's display of ads stems from its relationship with the advertisers. As a consequence, AdWords is no longer a neutral information vehicle: Google has a direct interest in internet users clicking on the ads' links (as opposed to the natural results presented by the search engine)". [168]

In a recent CJEU decision, the Court noted that "the mere fact that the operator of an online marketplace stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers cannot have the effect of denying it the exemptions from liability provided for by Directive 2000/31".[169] The Court then clarified that an intermediary service provider should not be able to rely on the exemption when it adopts "an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale", nor "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously".[170]

In practice, this has led to establishing the so-called "notice and take-down" procedures, meaning that owners of Intellectual Property Rights can directly notify a CSP, who will then have to remove expeditiously the infringing content from its platform/infrastructure. To deter-

[167] See CJEU judgement in Google France and Google, para 120.
[168] See Opinion of the AG, on Google France and Google, paras 143 and 144; nonetheless, the results presented by Google's search engine may be neutral concerning the treatment of data, even though it has been established that results usually vary from person to person, based on previous searches, age, location, etc…
[169] See judgement of 12 July 2011, L'Oréal and Others, Case C-324/09, ECLI:EU:C:2011:474, para 115.
[170] See CJEU judgement in L'Oréal and Others, paras 116 and 124.

mine the applicable law, the E-Commerce Directive considers that the place of establishment as the place where the firm has its center of activity.

3.2.5 Consumer Rights Directive

In accordance with the CRD,[171] where products and services are offered to consumers, without the simultaneous physical presence of the trader and the consumer[172] the provisions on distance-selling laws will further apply. Thus, the CRD will apply to a CSP when offering services to consumers, which will fall under the concept of digital services. Nonetheless, the definition of consumer in the scope of the provision of CSP, in light of the mixed uses that these allow, is less than straightforward.[173] In accordance to Cunningham and Reed, the conclusions of CJEU in case C-464/01, [174] even if referring to procedural elements and not substantive law, "cannot be denied and, further, the legitimacy of the decision for the purposes of substantive consumer law has been proven by the inclusion of the essence of the decision in the Consumer Rights Directive definition of consumer",[175] in recital 17 CRD. Thus, where a natural person contracts cloud computing services for a purpose which is outside its trade, business, craft or profession, it will be able to avail of the wide scope of protection granted by the CRD; also, considering that consumers will typically have no possibility to negotiate the Terms and Conditions provided by CSPs, they may even avail of legal protection provided under the Unfair Contract Terms Directive (UCTD)[176]. Nonetheless, even though this clarification is helpful, we consider that it will still be difficult to establish when a trade purpose is so limited as to lead to a consumer use; one potential solution that cloud service providers may consider is to clarify the main purpose of use of the services prior to concluding a contract with a new client.

---

[171] See note 65.

[172] Art. 2 (1) CRD provides that "'consumer' means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession." However, the notion is not unequivocal, see *infra*.

[173] See Cunningham, Alan and Reed, Chris, *Caveat Consumer? – Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud,* 2013, Queen Mary School of Law Legal Studies Research Paper No. 130/2013 (available at: http://ssrn.com/abstract=2202758) and Cunningham, Alan and Reed, Chris, *Caveat Consumer? – Consumer Protection and Cloud Computing Part 2 – The Application of ex ante and ex post Consumer Protection Law in the Cloud*, 2013, Queen Mary School of Law Legal Studies Research Paper No. 133/2013 (available at: http://ssrn.com/abstract=2212051).

[174] See judgement of 20 January 2005, Gruber. Case C-464/01, ECLI:EU:C:2005:32; the CJEU confirmed in para 54 of its judgement that a "a person who concludes a contract for goods intended for purposes which are in part within and in part outside his trade or profession may not rely on the special rules of jurisdiction laid down in Art. 13 to 15 of the Convention, unless the trade or professional purpose is so limited as to be negligible in the overall context of the supply, the fact that the private element is predominant being irrelevant in that respect".

[175] Op. cit. in note 173.

[176] See Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, as amended by Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 and by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019. More information this on note 173.

In the cases where a client is considered a consumer in the terms of the CRD, informational and formal requirements for distance or off-premise contracts need to be observed, namely the following: (i) main characteristics of the goods/services, (ii) the identity of the trader (i.e. at least, its trading name, address and phone number), (iii) if the trader is acting on behalf of another trader, the identity of the other trader must be provided, (iv) arrangements for payment, delivery and performance, the time by which the trader undertakes to provide the goods/services and its complaint handling policy, (v) price and duration of the contract and, if the duration is undetermined, the conditions to terminate the contract, etc. Lastly, CSPs shall consider that, under the updated CRD, consumers will avail from a right of withdrawal (Art. 9 CRD), which includes the consumer's right to retrieve any digital content it generated or provided, free of charge, within a reasonable time and in a commonly used and machine-readable format (Art. 13(7) CRD)

Lastly, Art. 25 of the CRD enforces the imperative nature of the Directive, indicating that consumers may not waive any right conferred under this Directive and that any contractual terms, which may result in a waiver or limitation to those rights, either directly or indirectly, shall not be binding on the consumer.

It should also be noted that the concept of "a trader acting on behalf of another trader" (i.e. platform providers with marketplace functionalities), as provided in Art. 6 (c) CRD, is not particularly clear. The responsibility of such marketplace platform appears to have been broadened by the European Commission Directorate-General for Justice (DG Justice), in its Guidance Document concerning the CRD, which indicates that "the provider of that platform shares, in so far as he is acting in the name of or on behalf of that trader, the responsibility for ensuring compliance with the Directive".[177] Should one accept such understanding, not only the party offering products and services on an online marketplace, but also the operator of such online marketplace will be required to comply with the provisions of the Directive,[178] which seems to raise new

[177] DG Justice Guidance Document concerning Directive 2011/83/EU, June 2014, p. 31. However, this appears to be somehow odd, since in page 24, the same document states that "where the trader provides an on-line trading platform for other traders to market their products, (…) the platform provider should make sure, through appropriate arrangements with the developers, that information about them as content providers is duly displayed", which seems to enforce the idea that platform providers would only need to indicate the identity and geographical address of the principal trader.

[178] As such, before finalising the purchase, the platform operator is bound to provide, on a durable medium, further information at least on the characteristics and the total price of the goods or services, the duration of the contract and the minimum duration of the consumer's obligations, if applicable. Accordingly, not only the party offering products and services on an online marketplace, but also the operator of the online marketplace is obliged to comply with the Directive. As such, before finalising the purchase, the platform operator is bound to provide, on a durable medium, further information at least on the characteristics and the total price of the goods or services, the duration of the contract and the minimum duration of the consumer's obligations, if applicable, as per Art. 6 and 8 of the CRD.

questions concerning intermediaries.[179] However, we note that the opinion of DG Justice is not legally binding nor does it provide a formal interpretation of EU Law and, as such, national transpositions may not follow the logic therein presented.[180]

3.2.6 Digital Content Directive

The DCD will apply to any consumer contracts for the supply of digital content or digital services; additionally, the DCD will apply when a consumer provides its personal data as "payment" in return of such digital content or services (Art. 2 (1) DCD)[181]; outside of the material scope of the DCD are services other than digital ones, electronic communication services, digital content made available to the general public, and software offered under a free and open-source license, as well as healthcare, gambling and financial services. .

The DCD also provides clarity on the requirements to demonstrate conformity of the digital content or service, namely that such will be fit for the purposes for which a similar type of content or service would be normally used, including its functionality, interoperability and other performance features (Arts. 6 to 10 DCD).

According to the DCD, traders must provide the acquired digital content/services, immediately after the conclusion of the contract, unless otherwise agreed with the customer (Art. 5). Should the trader fail to supply the content/services, the consumer shall call upon the trader to supply such content/services without undue delay; should the trader fail again to supply such content/services, the consumer shall be entitled to terminate the contract immediately; alternatively, and should specific time of supply be essential for the customer and the trader fails to supply the content/services in time, the consumer shall be entitled to immediate termination, in circumvention of the mechanism above. Lastly, the consumer shall be entitled to have such digital content brought into conformity with the contract, unless such is impossible, disproportionate or unlawful, or to receive a proportionate reduction in the price (Art. 14).

According to the DCD, any lack of conformity which becomes apparent within one year upon delivery/supply shall be presumed to have existed at the time of delivery for contracts providing for a single act of supply or a series of individual acts of supply (Art. 11 (2) DCD); furthermore, for digital contents/services, where the contract provide for a continuous supply,

[179] Please refer to Wendehorst, Christiane, *Platform Intermediary Services and Duties under the E-Commerce Directive and the Consumer Rights Directive,* Journal of European Consumer and Market Law, 2016, Issue 1, pp- 30-33.
[180] As clearly indicated in page 1 of the DG Justice Guidance Document, see note 177.
[181] An exception to the application of the DCD will, nonetheless, apply when the data have been collected solely for meeting legal requirements.

the burden of proof shall be on the trader for the duration of such contract (Art. 11(3) DCD); however, such distribution of the burden of proof will not apply, if the trader demonstrates that the consumer's digital environment is not compatible with the technical requirements, of which the trader has informed the consumer in a clear and comprehensible manner before the conclusion of the contract (Art. 15 (4) DCD).[182]. Traders are further obliged to inform consumers and to provide updates required to maintain conformity and security throughout the duration of the contract.

Additionally, the DCD provides guidelines regarding contract modification, termination of long-term contracts, the retrieval of data upon termination and the modification of digital content/services by the trader[183]. Lastly, it is also worth noting that, should any provision of the DCD conflict with another EU act, the other provision shall take precedence and that the application of this Directive shall not hamper the protection of personal data (Art. 3 (7) and (8) DCD).

3.3 Conclusions

As evidenced by the above assessment, the legal framework applicable to CSPs is very fragmented and fairly complex; the current information dispersion is further hindered by uncertainties on crucial elements, by the rapid technological evolution and by the multiple potential cloud arrangements. As such, there is a risk that medium or small CSPs, may find themselves overwhelmed by the several regulations and question how to achieve and maintain compliance to those obligations; a situation which might also impact their customers downstream. Accordingly, in its pursuit to accommodate innovation, some legislative texts seem to have introduced overly broad concepts which are difficult to operationalize and to integrate in a coherent manner (e.g. processing).

The above in no way disregards the fact that solid principles exist and provide guidelines to ensure security, integrity and destruction of personal data, the maintenance of consumers' trust and the continuous development of the internal market; however, further steps are re-

[182] For more information, please refer to Art. 9 and 10 DCD.

[183] In contracts supplied over a period of time, any provision determining that the supplier may alter functionality, interoperability and other features, in a manner which adversely affects access or use of the digital content by the consumer, can only occur if: (i) the contract so stipulates it, (ii) if the consumer is notified with reasonable advance in a durable medium, (iii) and if the consumer is allowed to terminate the contract, free of charges, within less than 30 days from receipt of the notice. Also, if the customer decides to terminate the contract under this article, it shall be provided with technical means to recover all content provided. For more information, please refer to Art. 15 DCD.

quired. Namely, there appears to exist an incorrect understanding that CSPs should be aware of which type of data they process – a perspective which is disconnected with how parties to a cloud computing operate; a potential alternative, as suggested by some, would be to consider some CSPs as neutral intermediaries, to the extent that data at rest is automatically anonymized, with the encryption keys not being provided to CSPs wishing to avail from such status.

Additionally, with the aim to increase transparency and to provide a more playing field, the introduction of model clauses for CSPs, depending on the type should be considered;. Lastly, further importance should be given to the introduction of mechanisms enforcing system interoperability and data portability, as these will lead to more balanced relationships between the Parties and more competition in the market, which in turn may increase consumer trust and to improve levels of service.

PART 4 – ANALYSIS OF "STANDARD" TERMS IN CLOUD COMPUTING AGREEMENTS

This chapter will focus on a set of Terms of Service (henceforth "ToS") of various cloud actors, following the assessment of various cloud computing agreements from diverse cloud actors (as indicated in Annex I to this thesis) which were available online, being offered to prospective customers and, hence, not subject to any alteration or negotiation. [184] The analysis undertaken in this chapter took into consideration the work conducted by Bradshaw, Millard, and Walden, with the objective of visualising the evolution and trends in this sector; therefore when possible, the same services/actors were assessed, while services within the same segment where used when such actors/services no longer existed.[185] As such, an overview of these agreements is provided below, segmented into four sub-sections concerning contractual aspects, data related matters, security obligations and liability/responsibility.

.For precision, we would like to clarify that we will use the term ToS to refer to the document establishing the main terms the relationship between the CSP and the customer; such designation will be used broadly and may, at times, include additional documents provided by the CSP, which may include the following:

- **Terms of Service (ToS)** – establishes the essential aspects of the relationship between the parties and usually includes the other documents by reference;
- **Service Level Agreement (SLA)** – as the name describes it provides for the expected level of service – be it uptime, bandwidth, number of connections supported, etc. – and the corresponding penalties/compensations in case of underperformance; given its nature, it is almost exclusively associated with paid services;
- **Acceptable Use Policy (AUP)** – establishes the restricted or allowed uses of the services provided by the CSP;
- **Privacy Policy** – indicates how the CSP will use and protect the customer's personal information, which may include provisions relating to data protection.

Furthermore, one should be aware that it is not uncommon for the abovementioned documents to be lumped together, namely joining the ToS and the AUP; also, as indicated above, for its nature, SLA's will usually be associated with paid services. Also, it is worth noting that all

[184] The list of ToS assessed are provided in Annex I and pertain to the ToS in place in May 2017.
[185] Please refer to Bradshaw, S., Millard, C. and Walden I., *Standard Contracts for Cloud Services*, in *Cloud Computing Law*, edited by Christopher Millard, Oxford University Press, 2013 pp. 39-72.

cloud services assessed had associated privacy policies, applying to all services provided by the CSP (and not only to the specific cloud service being offered), which could indicate that such issue is perceived more from a compliance perspective, than as a contractual matter.

Finally, prior to commencing the analysis of the standard contractual terms in cloud agreements, it should be clarify that the enforceability of some of the contractual terms[186] indicated below is controversial, especially in relation to individual consumers due to the special protection from which they avail, bearing in mind the broadening of the consumer concept discussed above.[187] Due to restrictions relating to the length and theme of this thesis, such topics will not be assessed in detail, however, information will be provided when clauses are deemed void or invalid, when dealing with consumers, where relevant.

4.1 Contractual matters

4.1.1 Duration and consideration

Firstly, a line should be drawn to distinguish free and paid cloud computing services; as such, we note that a ToS for paid services usually indicates the initial term, the renewal mechanism and the associated payment structure – the rule in most is that the contract will be in place continuously, until it is terminated by one of the parties.[188] On the other hand, free services will usually have no fixed contract term; however, to avoid unlimited obligations, CSP may (and usually will) have provisions in place designed to excused itself from continuing offering the free services, in case of breaches to the APU or in case of lack of use of the service.[189]

More than half of the assessed ToS provide for free services, with most of them foreseeing associated costs for extra/premium features (more storage, access to software, no advertising, etc.). However, as advanced by Metafilter user blue_beetle, "if you are not paying for it (…)

---

[186] Some of disputed enforceable terms include provisions on jurisdiction and choice of law, unilateral variation of contract terms, termination and suspension and limitation of liability. For more information, please refer to Alan Cunningham and Chris Reed *Consumer Protection in Cloud Environments*, in *Cloud Computing Law*, edited by Christopher Millard, Oxford University Press, 2013 pp. 331-361; and to *Consumer law compliance review: cloud storage – findings report*, Competition & Markets Authority, May 2016; available at: https://assets.digital.cabinet-office.gov.uk/media/57472953e5274a037500000d/cloud-storage-findings-report.pdf, last accessed on 26/04/2020. Also, see the Bureau Europeén des Unions de Consommateurs' (BEUC) contribution to the European Commission's Export Group on Cloud Computing Contracts, regarding Unfair Contract Terms in Cloud Computing Service Contracts; available at: http://www.beuc.eu/publications/beuc-x-2014-034_are_ec_expert_group_on_cloud_computing_contracts.pdf, last accessed on 26/04/2020.

[187] Please see section 3.2.6 (CRD).

[188] See AWS ToS: "The term of this Agreement will commence on the Effective Date and will remain in effect until terminated under this Section 7."

[189] See Dropbox ToS: "We reserve the right to suspend or terminate your access to the Services with notice to you if: (…) (c) you don't have a Paid Account and haven't accessed our Services for 12 consecutive months."

you're the product being sold"[190], as such, those free services will generally have hidden costs. Most free services will rely on contextual advertising to generate profits, while others will use personal data, user information and browsing habits to provide users targeted advertising or to conduct marketing analysis. In some cases, services will also require the provision of an associated licence to use content hosted/shared by the user[191], without any form of compensation for the user. This issue should be carefully addressed since in some cases the scope and duration of the licences will be very broad and may seriously impact users and future business applications of ideas shared/hosted in the Cloud. In this matter, higher transparency concerning the reach of these licenses would be a welcome change on the part of CSPs, which could likely decrease the fear of losing control over hosted content – one of the main obstacles to cloud computing adoption.[192]

4.1.2 Applicable law and jurisdiction

According to my analysis, most ToS indicate their local law as governing and their own jurisdiction as the correct forum; in one case, the ToS provided for no specific law[193]. It should be, noted that CSPs appear to be attempting to accommodate to the EU legal framework; specifically, one-third of the assessed ToS provide for possibility to refer to the courts of the user's country of residence, as well as the application of the laws of the country of the user in some cases.

In relation to the remaining two-thirds of assessed ToS, it appears that CSPs did not consider the provision of the Rome I Regulation[194] and of the Recast Brussels Regulation[195], on consumer contracts.

As such, concerning consumer contracts, the law of the country where the consumer habitually resides, shall govern the contract, insofar as the CSP pursues activities in such country or

[190] See http://www.metafilter.com/95152/Userdriven-discontent#32560467 (last accessed on 26/04/2020).
[191] See Google Drive ToS: "You give Google a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our services, and to develop new ones. This license continues even if you stop using our services unless you delete your content." This happens mainly for free services; however, some paid services also request the provision of a licence to distribute/share user content.
[192] See section 2.5.2.
[193] See Basecamp ToS; however, following an email, Basecamp informed us that "our jurisdiction is the place where Basecamp has its central administration and/or services, which in our case are all in the US".
[194] Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).
[195] Regulation (EU) no 1215/2012 of the European Parliament and of the Council of 12 December 2012.

if it directs activities towards such country (see Art. 5(1) Rome I Regulation); however, a provision regarding choice of law may still be enforceable in consumer contracts[196] only if it does not deprive the consumer of any mandatory provisions of the consumer's habitual residence (see Art. 5(2) Rome I Regulation).

In what concerns jurisdiction, regardless of the ToS consumers may bring proceeding against the suppliers in the courts of the place of their habitual residence (Art. 18(1) Recast Brussels Regulation); in addition, a professional intending to bring a proceeding against a consumer may only do so in the courts of the country where the consumer's habitually resides. Additionally, considering that such clauses are not individually negotiated it may be regarded as unfair under the UCTD if it causes significant imbalance between the parties' rights.

This should be a point of relevant concern to CSPs given that many end-users of cloud services are consumers, who will be entitled to a greater degree of legal protection when entering such contracts, namely pertaining to the selection of applicable law in non-negotiable ToS, which may easily be considered void; as such, recognition of local/regional legislation should be considered by CSPs.

Regarding B2B, the parties are free to determine jurisdiction and applicable law, under certain limitations (e.g. in case of domestic contractual situations and if not overriding mandatory provisions, respectively).

Furthermore, it is also worth noting that some CSPs provide for the use of arbitration[197], as well as other alternative dispute resolution mechanisms[198]. Differentiated approaches also exist, e.g. Microsoft's ToS relate to the laws of Washington State, when concerning cost-free services, while, for paid services, the governing law will be that of user's habitual residence.[199]

---

[196] This issue is addressed by Cunningham and Reed, see op. cit. in note 186.

[197] See AWS and ADrive ToS. It should also be noted that such clauses will likely not bound consumers, given that both are manifestly against Annex I, line q) of the Unfair Contract Terms Directive; as such, these clauses would only be enforceable towards consumers if the CSPs can demonstrate that such particular condition was clearly brought to the attention of that party. For more information on this topic, please refer to Bucilla, JR, "'The Online Crossroads of Website Terms of Service Agreements and Consumer Protection: An Empirical Study of Arbitration Clauses in the Terms Of Service Agreements for the Top 100 Websites Viewed in the United States"', Wake Forest Journal of Business and Intellectual Property Law, Vol 15, 2014.

[198] In its ToS, Dropbox indicates that before filing a legal claim, the user agrees to try to informally resolve the dispute with Dropbox. Google Drive indicates that disputes may also be submitted to the European Commission Online Dispute Resolution platform.

[199] As per the DG Justice Guidance document (see note 177), the current CRD does not seem to apply to gifts or services provided for free concerning sales and service contracts, even though it would apply in cases of contracts for the supply of online digital content. As such, the approach by Microsoft may not be void. From my part, the assessment in the aforementioned Guidance Document seems to disregard the notion that the absence of a price, reflected in a monetary amount, will not in most cases amount to the absence of a consideration, given that "free" online services have relied on the possibility to use (and in some cases share and sell) the personal data provided by the user to further market its products (or those of other entities). As such, a consideration is provided by the con-

4.1.3 Acceptable use policies (AUP)

AUPs tend to restrict/limit the applications/uses that users make of the available cloud computing services. All assessed services included some sort of AUPs, either included in the ToS or in a separate document. Regardless of their length or scope, these clauses will usually have a broad scope, including illegal, harmful and fraudulent activities, violations of third-party content (IPR), offensive or harmful content, security violations, network interference, email or message abuse (i.e. spam, phishing)[200]. Some CSPs have also included restrictions on the storage of data from/export of data to Cuba, Iran, Iraq, Libya, North Korea, Syria or Sudan (or to/by a national or resident of those countries)[201] or limit the use of service to only "person non-commercial purposes";[202] while others indicate that the use of distributed, peer to peer network services (i.e. Tor) are allowed. Users should analyse these terms since these will often include relevant clauses and breach thereof may result in immediate termination (and potentially loss of data associated with such account).[203]

4.1.4 Termination

The grounds for termination may have particular importance depending on the criticality of the service, specifically if termination may happen immediately, without the possibility of further access to content/infrastructure by the user (i.e. retrieval of data).[204] Accordingly, we present below the most common termination provisions in the ToS we assessed.

The termination of the services may be brought by either party, either by convenience or for cause. In case of users of paid services, termination may either have immediate effect or re-

sumer, even if such does not a specified monetary value; hence, the customer should not see its rights diminished for the absence of a monetary consideration. Such understanding is also defended by McGillivray, K., in "A right too far? Requiring cloud service providers to deliver adequate data security to consumers", International Journal of Law and Information Technology, 2017, Vol. 25, Issue 1, pp. 9-11. Such level of protection has been lately endorsed by the European Commission in COM (2018) 183 – A New Deal For Consumers.

[200] Except for Basecamp, which only stated that "You may not use the Service for any illegal purpose or to violate any laws" and that "Verbal, physical, written or other abuse (…) of any Service customer, Company employee or officer will result in immediate account termination".

[201] See ADrive ToS.

[202] See Google Drive ToS.

[203] The applicability of these terms was assessed by the English High Court in the case of "Overy v PayPal (Europe) Ltd", when PayPal intended to enforce the terms included in its AUP, which prevented the use of its services for lottery or gambling activities.

[204] See section 4.2.4

quire a 30 days' notice period, while for users of free services, termination may be requested at any time, with immediate effect.[205]

For CSPs, the majority of the assessed ToS establish that if it decides to terminate a user account/service, and no wrongdoing occurs, then, such termination may be preceded by a notice period, allowing the user to transfer/retrieve its' content or migrate its structure/application. However, if a user is in material breach or has repeatedly violated the ToS/AUP, or if its' activity is likely to cause legal liability to the CSP or compromise its ability to provide service, CSPs have the prerogative to terminate the service without any type of notice, which, even though it may seem extreme, is a common and widely accepted approach in view of other higher concerns, such as the protection of the network, the services and the internet in general. Also, users should be especially aware that some ToS provide for immediate termination, for any reason, at any time,[206] given the impact that such may have on them or those that may relate to circumstances not fully under their control.[207] Lastly, concerning ToS for free cloud services, those may also include termination clauses for inactivity.[208]

In this context, it is worth highlighting that provisions enabling a CSP to terminate consumer contracts with an indeterminate duration without reasonable notice will also be considered unfair under the UCTD[209], unless there are serious grounds to do so.

4.1.5 Variation of contract terms

All ToS mentioned the possibility of alteration to the terms of the contract, even if such reference is minor.[210] A large majority, indicate the date when they were last updated, with only three ToS not providing such information and one indicating a version number.[211] Additionally, we noted that two CSPs include in their websites a historic of the alterations introduced, while

[205] E.g. Dropbox ToS "You're free to stop using our Services at any time".
[206] See ToS for 500px, Basecamp, Instagram and Linode.com – Linode, however, states that it will use "reasonable care in notifying the Customer", even though such is not assured. In light of this, we contacted Linode, which indicated that "Linode does reserve the right to terminate any customers services at any time. We reserve this right as a way to maintain the safety and integrity of our infrastructure for our entire customer base.".
[207] E.g. Linode ToS, section 10, provides a termination right to Linode following the receipt of a valid Court Order to disclose data on the user's account, which some clients may consider as an excessively risky provision, given that such Court Order may not relate to a unlawful or unauthorised or its claims may end being unfounded.
[208] See ToS for Mega (3 months), Dropbox and iCloud (both 1 year), PayPal (3 years), and Microsoft (5 years).
[209] See Annex n.1, line g) UCTD.
[210] See Basecamp ToS, which only indicates that "The Company reserves the right at any time and from time to time to modify or discontinue, temporarily or permanently, any part of the Service with or without notice."
[211] See ToS For 500px, Basecamp, Linode.com and Norton Online Backup – the last indicated "TOS 2.1", which we assume relates to the version of the document.

one provided the previous version[212] – these are welcomed changes, since they allow users to assess the changes undertaken and consider the evolution of the ToS, as a living document.

The modification of the terms is usually a unilateral prerogative of CSPs[213], which in most cases commit to notify users of alterations to the ToS, SLAs, description of services or pricing;[214] such notification will, in circa 50% of the assessed ToS, consist in the mere upload of a new ToS to the website.[215] Modifications will become effective in the terms defined in the ToS or in the notification itself, but it will usually give a 30 days period to object to the amendment or to request termination of the services, should such be established in the ToS.[216] Also, the majority of assessed ToS, CSPs indicate that the continued use of the services, after their effective date, will constitute acceptance of the terms. However, specific and limited circumstances, relating to maintenance of security and operability of services, prevention of abuse or compliance with legal requirements, may entail the need to insert alterations without notice.[217] It is also worth noting that some services will provide Users refund of any paid unused amounts when termination occurs due to an amendment of the ToS.[218]

In clear opposition to the above, Norton Online Backup was the only service not undertaking unilateral changes and indicating that no amendment to its "Agreement will be binding unless evidenced by a writing signed by the party against whom it is sought to be enforced", nonetheless it asserts sole discretion to amend general operating practices.

In this sense, it should be noted that provisions allowing the CSP to unilaterally introduce either alterations to the contract without a valid reason (as specified in the contract) or alterations to the characteristics of the service being rendered, will be considered unfair in consumer contracts.[219]

---

[212] AWS and Microsoft allow users to consult the changes inserted to the documents, while Instagram provided the previous version of its Terms of Use.

[213] The enforceability of provisions allowing for unilateral alteration of contract terms when dealing with consumers is also unlikely, in the light of lines j) and k) of Annex I of the UCTD. Such interpretation was taken by Berlin's Regional Court, in relation to a claim brought by the German Consumer Association VZGV, against Google (Landegericht Berlin, case no. 15 O 402/12,).

[214] Only Basecamp ToS is silence on notification of changes.

[215] As per the Terms of Use of Instagram; "You agree that we may notify you of the Updated Terms by posting them on the Service, and that your use of the Service after the effective date of the Updated Terms (or engaging in such other conduct as we may reasonably specify) constitutes your agreement to the Updated Terms." Similarly, the ToS for 500px, AWS, PayPal

[216] See ToS for AWS, Datapipe (former GoGrid), Dropbox, Google Drive, iCloud, MEGA, Microsoft and PayPal. However, please note that some of these CSPs will exclude documents such as Privacy Policies, SLAs or AUPs from this notification period, with changes being immediate in some cases (e.g. Datapipe).

[217] See Google Drive ToS, section 7.

[218] E.g.Dropbox ToS.

[219] See Annex n.1, line j) and k) UCTD.

Also, during the assessment it was noted that many CSPs provide their ToS in more than one language, usually relying on the English version in case of discrepancies or conflicting regulations; in this case, could such clause be fully enforceable, if, during signup, a user is provided with a ToS in its own language which has not been updated to match its English version? In other words, is it reasonable to impose on the client the burden of reviewing the ToS in the English language to ensure coherence with the version being presented? This idiosyncrasy was present when we assessed the AWS ToS and attempted to create an account using Portuguese as the default language; in this case, we were provided with a document from December 2011, which bears little resemblance to its current English version. In relation to contracts with consumers, a reply to these questions is found in the UCTD, which, in line with a *pro consumatore* interpretation, establishes that "where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail".[220]

4.2 Data and security matters

4.2.1 Integrity and data preservation

The approach to integrity[221] referred to Bradshaw, Millard and Walden[222] has not been widely altered, with most assessed ToS disclaiming integrity of data all together and the remaining not even establishing any provision on the matter. Even though CSPs state that they "will make reasonable efforts to recover data lost", that they employ "industry-standard technical safeguards",[223] or that their "systems are engineered to stay up even if multiple servers fail"[224] or offer backup services, CSPs still included numerous and comprehensive disclaimers on this matter.[225] In this context, it is thus clear that those indications seem far too empty and are concerning for both experienced and untried customers, for the former because it will provide them little assurance concerning their data, while to the latter it may provide a false sense their data is secure. Accordingly, further steps must be given to promoting consumer trust, either by providing evident information that data stored, even in backup services, is not fully ensured. Also, it is also worth noting that under the GDPR CSPs will have to notify the competent Data Protection Au-

[220] See Art. 5 UCTD.
[221] For the purposes of this subchapter, integrity shall relate to the securing of data against illicit alteration, loss or destruction.
[222] See note 185.
[223] See Datapipe ToS.
[224] See Basecamp Security Overview: https://basecamp.com/about/policies/security (last accessed on 26/04/2020).
[225] E.g. Datapipe ToS: "Customer is responsible for maintaining security, including disaster recovery systems and backups. (Customer is advised to maintain its own backups outside of GoGrid's premises and systems, even if GoGrid provides backups, security, or other services related to data protection.)"

thority in the event of personal data breaches, as well as the data subjects in some cases.[226] However, the assessed ToS do not reflect such upcoming legal alterations and also do not ensure notification if breaches occur. In light of the above, it is also debatable whether a complete disclaimer on the integrity of data in a consumer contract would not be deemed unfair, especially when providing storage/back-up services.[227]

Concerning data preservation[228], the provisions adopted by CSPs on this issue vary significantly; however, CSPs usually offer one of the following outcomes:

- Deletion of all content upon termination;[229]
- Maintenance of data only for a set period of time after termination, then, deletion;[230]
- Absence of a firm commitment to deletion (i.e. "may delete");[231]
- Maintenance of data after termination.[232]

Of the surveyed ToS, approximately 40% of the CSPs allowed users to retrieve content after termination under certain circumstances. 30% opted for the first option and 25% chose the third, with only one provider indicating that it would maintain data.

Concerning maintenance of data after termination, it is also worth mentioning that Facebook included a feature allowing either the memorialisation of accounts in case of a user's death, preserving the content and allowing limited comment on the account.[233]

Lastly, we would like to highlight that the issue of data preservation/deletion should be addressed with specific care in cases where cloud users deal/handle sensitive data, given that it will be in their best interest to ensure that such is fully removed from storage, once its agreement with the CSP is terminated. Additionally, such issue may also be subject of concern for CSPs, given that they may assume responsibility for the security of dormant/non-deleted personal data submitted by its users – it is also relevant to remember that different levels of "deletion" exist

[226] See Art. 33 and 34 of the GDPR.
[227] See Annex, n. 1, line b) UCTD; such type of provision could in any case be framed as unfair, as per Art. 3(1) UCTD, for introducing a significant imbalance in the parties obligations to the detriment of the consumer.
[228] For the purposes of this subchapter, this concept relates to whether services take appropriate measures to ensure that following termination (regardless of the possibility of retrieval), data is duly deleted.
[229] E.g. 500px ToS: "Upon termination of your account 500px will automatically remove all Visual Content posted to your account."
[230] E.g. Google Drive ToS: "If we discontinue a Service, where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service."
[231] E.g. ADrive ToS: "ADrive may, but shall not be required to, delete Your Storage Data after the termination of this Agreement."
[232] E.g. PayPal ToS: "If you close your PayPal account, we will mark your account in our database as "Closed", but will keep your Account Information in our database."
[233] See Memorialized Accounts, https://www.facebook.com/help/1506822589577997/ (last accessed 26/04/2020).

and more secure deletion techniques (i.e. overwriting or replacing or destruction of hardware) will be more expensive.[234]

4.2.2 Retrieval of data upon termination and lock-in

The majority of surveyed ToS do not provide for retrieval of content upon termination, regardless whether such termination was motivated by discontinuation of service, lack of payment or violation of AUP, terms or law. The CSPs that foresee the possibility users to retrieve content do so with constraints as well, usually allowing for a reasonable period for data to be retrieved. This is a positive evolution; however, further steps should be given, namely including terms to ensure interoperability of services, by providing data/content in a commonly used data format allowing users to change providers swiftly and without incurring in significant costs; in a nutshell, preventing user lock-in, which is still not addressed in any of the surveyed agreements, but that remains, as indicated in section 2.5.2, as one of the major risks perceived by users when moving into the cloud.

Lastly, it should be noted that during the drafting of this thesis, the DCD has been approved and established that, upon termination, traders will have to allow consumers to have access any content provided when using the trader's content/services;[235] hence, it is expected that CSPs will adjust their ToS, accordingly. Such changes may further contribute to an increase in competition between cloud services and enable the emergence of competitors in fields where competition is marginal or inexistent, in addition to promoting consumer choice.[236]

4.2.3 Disclosure and confidentiality of hosted data

This subchapter relates to the circumstances in which CSPs may or will disclose user information. According to the analysed ToS, different approaches have been adopted, depending on how strictly CSPs commit to ensuring the confidentiality of hosted data. Some providers, such as ADrive, have a very low threshold for disclosing information to law enforcement and proper authorities, doing so if it believes "in its sole and absolute discretion" that you may be

[234] The GDPR does not clearly explain what type of deletion of personal data has to be ensured, however, I consider that its ratio would be significantly hampered if data is merely left "dormant". Also, the controller's option to have the personal data either deleted or returned seems to point to a permanent deletion of data (see Art 28, 3. (g) GDPR).
[235] Furthermore consumers shall be entitled to retrieve such content be free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format (Art. 16 (4) DCD).
[236] The potenital impact of Art. 20 GDPR, concerning data portability, is still absent from the assessed ToS, even though most of the assessed CSPs will be required to observe it.

engaging in unlawful or improper activity. Similarly, also Apple states that it will disclose Account Information and Content to law enforcement authorities, government officials and third parties, if it believes that such is reasonably necessary. On the other hand, Basecamp clearly states that disclosure will only occur upon receipt "a lawful request by public authorities",[237] in most cases, providers establish that disclosure will happen to prevent fraud or illegal activity or violation of the service's terms. Some providers indicate that, if not prohibited by law, they will inform the user of such request and provide "reasonable assistance at the Disclosing Party's cost".[238] In the case of social networks, such as Facebook and Instagram, these also include the prevention of imminent bodily harm as grounds for disclosure.[239]

Another two elements are worth mentioning. One is Dropbox's Government Data Request Principles,[240] which promote transparency and fight overly broad requests, in order to build trust on their services, while protecting all users. The other is the user controlled encryption mechanism included in MEGA's service, which increases users' trust in the service, given that "user's data is encrypted by the user before upload to our system and therefore we do not and cannot access that content unless we are provided with the decryption key".

4.2.4 Transfer and location

In the scope of this analysis, it is noted that some providers, such as Amazon and Linode,[241] allow users to choose where their data will be hosted; however, only Amazon incorporates in its ToS such ability to choose, in addition to committing to the maintenance of data in the selected location. On the other side, Linode allows the users to choose a specific location to host their data during sign-up, however, the ToS is silent on this matter, even though some may claim that such information is part of the representations made by Linode; additionally, Linode's ToS and website are both silent when whether data will be transferred to a different location,

[237] See Basecamp ToS.
[238] See Salesforce ToS.
[239] See ToS for Facebook and Instagram; concerning the latter, we note that the ToS, from 2013, states that "[n]one of your Content will be subject to any obligation of confidence (…), and Instagram will not be liable for any use or disclosure of any Content you provide"; since then Instagram has evolved and now includes a messaging service. Accordingly, we believe that such clause may leave some current Instagram users fairly unsettled. Furthermore, and bearing in mind that such services allow users to exchange private messages, doubts arise to whether such confidentiality may not be imposed to them, via the ePrivacy Directive transpositions.
[240] See https://www.dropbox.com/transparency/principles .
[241] Only Amazon indicates that ability to choose and to maintain data in the selected location its ToS. Linode allows the users to choose a specific location to host their data during sign-up, however, the ToS is silent on this matter, as well as to whether such data will be transferred to a different location. Concerning Datapipe, the website indicates that the company has several locations and allows users to choose any, however it also does not

however, its support services indicated that data will remain in the location initially chosen[242]. Lastly, we would like to highlight the case of Datapipe, since on its website it indicates several possible locations/data centres, which users are apparently allowed to choose from, however, such is not included in their ToS either; Datapipe does not provide any indication if data will be maintained in any specific location.

However, more than half of the surveyed services have no reference to location, while the ones that do so, usually will not make any reference to it in their ToS.[243]

Concerning the transfer of data, as we noted above, only one CSP committed to maintaining data at a selected location, which is surprisingly given the importance of this issue and the associated risks having data circulating in different areas – namely those where an adequate level of data protection mechanisms do not exist. However, we note that 70% of the surveyed providers indicated that they either are certified under the EU-US Privacy and/or rely on Model Contractual Clauses, a number which reflects the notion that compliance with the European framework may be decisive when choosing a CSP.

Another issue of some concern relates to the security of data in transit. During this assessment, we found that more than 70% of surveyed CSPs indicated that transferred data will be encrypted,[244] thereby decreasing the risk of in transit interception of data.

4.2.5 Data Protection

The issue of Data Protection is not a contractual but a regulatory one; however, this issue is intimately connected to that referred above, given that the GDPR prohibit transfers of personal data to countries outside the EEA unless such occurs under specified circumstances. Consequently, when acting as processors of personal data, CSPs would have to ensure compliance with such.

In light of that, most CSPs have ensured certification under the Privacy Shield and included Model Contractual Clauses[245] in their agreements with users. These steps accommodate users'

[242] According to Linode's email, it "won't move (…) data to another datacenter unless you request it, and it will remain in the same location until you remove the Linode in which case it'll be securely deleted. The one exception to this is if you create an image using our Images beta. In that case the image will be cached in each datacenter for more rapid deployment.".
[243] E.g. Basecamp indicated in an email that all of its servers are located in the US, however, such information is not provided publicly.
[244] However, even though some commit to encryption of all data transfers – e.g. Basecamp, Dropbox and MEGA –, other CSPs may only ensure such encryption in relation to passwords and personal or credit card information – e.g. iCloud, Microsoft, Norton Online Backup and PayPal.

obligations concerning both the limitation on transfer of data, as well as those relating to the flow-down of requirements to their processors (i.e. the CSPs). In doing so, CSPs – having/using data centres/servers outside the EEA – guaranteed that such processed data has a level of protection similar to the one it would enjoy in EU (and can be freely transferred) and that certain obligations and limitations will be observed, namely that processing will only be carried out in accordance with the instructions of the controller (i.e. the user). Thus, this is a positive step into ensuring compliance with data protection obligations of both processors and controllers.

However, CSPs may be controllers for other sets of data. Accordingly, it is important to notice that in this regard, all CSPs provide for some sort of Privacy Policy, which will generally include the following topics:

- What type of data is collected and how – at least including name and access data, however, may further contain location, demographic, payment, device and usage data, IP address, credentials, as well as contacts and relationships and the overall user content; content may be collected directly from the user or by cookies;[246]
- How/for what purposes the data will be used, including the legal basis for processing, details of the controller and of the data protection officer and the data subject's rights and how to exercise them;
- A general commitment not to share personally identifiable information (PII) – with the exception of social media platforms,[247] CSPs commit not to share any PII with third parties without consent;[248]
- The third parties which may receive information (i.e. authorised recipients) – usually CSPs retain a right to share data not containing PII,[249] such as metadata, aggregated demographic information, browsing habits, etc.;
- Access to user data – most Privacy Policies allow the user to access, correct or remove its data.[250]

---

[245] E.g. the Data Processing Addendum and corresponding Model Clauses by AWS, as well as Dropbox's EU Standard Clauses, based on Commission Decision 2010/87/EU; more info on this on note 123.
[246] On this matter, we note that Microsoft identifies some of the commonly used cookies in its Privacy Policy, indicating their purpose/function.
[247] However, when sharing data with third parties for advertising and analytics, Facebook will not share any PII with these entities, unless the user provides permission to do so.
[248] Exceptions to this are third party service providers, law enforcement agencies/authorities or in case of acquisition of the CSP. On this regard, we note that PayPal includes in its website a list in which it indicates all third parties financial/payment service providers to which it may disclose data, in a rare demonstration of transparency.
[249] Apple's Privacy Policy (applicable to iCloud) establishes that "We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose."; however, given the emergence of big data and the increasing amount of data and combination techniques, one wonders to which extent may such data be identifiable.

In addition to these standard terms, other relevant issues emerged in namely those relating to compliance with privacy/data protection frameworks, the maximum retention period of personal data and mechanisms assisting cross-border transfers of data. The provision of such information in a clear and simple manner is vital since it will allow users to better understand which information they are relinquishing and promoting better understanding of how information is shared.

4.2.6 Security measures & audit rights

Despite not guaranteeing data integrity, all CSPs will include some indication of security measures undertaken to reassure clients that their data is protected, indicating, at least, use of "commercially reasonable safeguards" or "enterprise-level security".[251]

As noted above, most CSPs provide encrypted data in transit, but may not guarantee encryption for data at rest.[252] However, such security measures do not only relate to the security of data but may also relate to the existence of accompanying certifications[253] or physical security of the sites where data is stored.[254] In this context, we note that depending on the service being offered, security measures associated will usually become more robust if such product involves the provision of payment details or sensitive information. It is also worth highlighting that the inclusion of additional security measures is usually not influenced by users, unless they represent a larger group of users, or if strict legal compliance mandates so.

Furthermore, one bizarre conclusion was made clear from the present analysis: none of the assessed ToS included a provision relating to notification of users in case of security breaches to their services/structures,[255] even though most ToS require users to "immediately notify (…) any unauthorized use of your account or any other security breach".[256] The absence of any reference to data breach notifications is very unusual since the GDPR obliges data processors to notify

---

[250] One exception to this is PayPal, which informed us that it will not delete user's data following cancellation.
[251] See ToS for Instagram and 500px, respectively.
[252] See Basecamp ToS "Data isn't encrypted while it's live in our database (since it needs to be ready to send to you when you need it), but we go to great lengths to secure your data at rest".
[253] Typical certifications include, but are not limited to, ISO 27001 (Information Security Management), ISO 27017 (Cloud Specific Controls), ISO 27018 (Personal Data Protection), as well as the Payment Card Industry Data Security Standard, SOC 1, 2 and 3, the CSA certifications, amongst others. ENISA provides an overview on this topic at: https://resilience.enisa.europa.eu/cloud-computing-certification (last accessed on 26/04/2020).
[254] See e.g. ToS for Datapipe, which indicates yearlong physical onsite security.
[255] The only noteworthy provision is included in the Microsoft Services Agreement, which only indicates that "When there's something important to tell you about a Service you use, we'll send you Service notifications and information the law requires us to provide", not clarifying if a security breach will be communicated.
[256] As per Linode's ToS. See also ADrive (ToS, section 4.), Dropbox (Business Agreement, section 2.2), iCloud (T&C, Section IV.A.).

data controllers, without undue delay, and obliges data controllers to notify data subjects when breaches are likely to result in a risk to their rights and freedoms;[257] a similar obligation which can also be found in Art. 4(3) ePrivacy Directive, when a breach is likely to affect the data subject's personal data. As such, one can only speculate if CSPs have disregarded this issue or whether consideration about it was left out due to its regulatory nature; either way, CSPs who fail to comply with those notifications, may see themselves on the end of the hefty sanctions foreseen by the GDPR.

Concerning audit possibilities, only Amazon allows limited penetration testing,[258] which aims to assess the resilience of the system and spot potentially weaknesses. Even though other CSPs do not allow users to audit their systems, most make available their certifications and accompanying reports publicly, which allow users to assess their systems' security, even if only to a certain level.[259] It is also worth noting that some CSPs, such as PayPal or Google,[260] have ongoing bug bounty programs, in which they invite professional researchers/ethical hackers to penetrate their systems or networks, with the purpose of finding security weaknesses that a malicious hacker could exploit.

Lastly, it should be highlighted that many of the existing privacy and security data risks, which are intrinsically connected with the inherently unbalanced consumer-CSP contractual relationship, could be addressed by the adoption of relevant international standards, as a mean of providing more transparent and consistent security practices.[261][262]

4.3 Liability matters

4.3.1 Guarantees

All of the scrutinised CSPs fully disclaim any type of guarantees (either legal or commercial – sometimes referred to as warranties in some ToS) associated to their services/product, indicating that the service is provided "as is", "as available", and "without warranties of any kind", in-

[257] See Art. 32(2), 33 and 34 GDPR.
[258] See https://aws.amazon.com/security/penetration-testing/ (last accessed on 26/04/2020).
[259] Nonetheless, it is worth noting that, under the GDPR, any processor-controller shall include provisions authorising the controller (or an auditor mandated by him) to conduct or contribute to audits and inspections to the processors in order to demonstrate the latter's compliance with its obligations.
[260] See https://hackerone.com/paypal and https://bughunter.withgoogle.com/, respectively (last accessed on 26/04/2020).
[261] For more information, please refer to de Hert, P., Papakonstantinou, V., and Kamara, I., "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection", in Computer Law & Security Review, Vol. 32, issue 1, pp. 16-30.
[262] For more information on the topic of data security in relation to consumers, please refer to McGillivray (op. cit. in footnote 199).

cluding those of merchantability or fitness for a specific purpose. However, it is also noticeable that in such attempt, CSPs directing their services to the European Union market have recognised the need to insert exceptions to those broad limitations[263] in the ToS, to adapt to European consumer protection rules, which limit the exclusion of legal guarantees.

Accordingly, differences in the scope of guarantee disclaimers will be predictable between an agreement which asserts the law and jurisdiction of the USA – generally broader – and one which commits to the law of an EU Member State.

In this sense, it should in any case also be noted that in the EU minimum (legal) guarantees apply to products or services marketed to consumers. As such, the likelihood of such provisions being deemed void in case of consumer's contracts is very high,[264] which would lead to the imposed recognition and application of a minimum conformity guarantee, on the basis of the expectations of an average consumer.

4.3.2 Exclusion and limitation of liability

The commentaries provided in the preceding subchapter are also applicable, almost *ipsis verbis*, to the approach that CSPs take to the exclusion of both direct and indirect liability. Such exclusions of liability are provided either in long statements, such as those in ADrive's ToS,[265] or in short ones, like that of Datapipe;[266] however, the intended result is the same: the exclusion of any liability by the CSP towards users, arising from the services/product. However, as indicated above, CSPs providing/directing their services to the European area will moderate these exclusions, in which cases these entities will recognise liability for (i) fraud or fraudulent misrepresentation in providing the services, (ii) negligence or wilful misconduct, (iii) death or personal injury resulting from negligence, as well as for any losses and damages (iv.a) that are a reasonably foreseeable result of the CSPs failure to use reasonable care and skill or (iv.b) that result from a breach of the CSPs contract with the user.[267]

[263] E.g. Microsoft Service Agreement: "If you are a consumer, you have certain rights under the law. These rights include an obligation on Microsoft to provide the Services using reasonable care and skill. Nothing in these terms is intended to limit or exclude our liability for any breach by Microsoft of this. Except in cases in which we have hidden defects in bad faith or defects have rendered use of the services impossible and except for skype paid products, we provide the services "as is," "with all faults" and "as available."'

[264] See note 227.

[265] See section 15 of Adrive ToS.

[266] See section 6.2, paragraph 1 of Datapipe ToS.

[267] E.g. ToS for Dropbox, iCloud and Google Drive.

In addition, regardless of whether the CSP limits the typical exclusions for direct and indirect liability, most CSPs[268] will also include monetary limitations/maximum caps on the amount of damages, which may range from 100 USD,[269] to the amount paid for the services in a certain period, which may in some cases mean zero.[270] One specific CSP adopts a hybrid approach, indicating that its liability – not accounting for liability which it cannot limit by law – will be the greater of 20 USD or 100% of the amount paid for the ongoing service plan.[271]

Regardless of the exclusions and limitations provided above, it should be noted that due to EU consumer protection law such provisions will not be valid in consumer contracts, to the extent that they go beyond the service performance, attempt to exclude unrelated types of damage (i.e. damage to computer system, loss of data), and/or inappropriately limit the legal rights of the consumer.[272] As such, there is a very high probability that such clauses are deemed void; consequently, in cases where CSPs exclude any type of guarantee of quality of service, or exclude liability without reasonable justifications or inappropriately limit monetary compensation, CSPs may be liable without limitation, for damages caused to European consumers.

4.3.3 Indemnification by the Customer

Despite establishing comprehensive limitations on their own liability towards users, CSPs require, nonetheless, that users defend, indemnify and hold them harmless from any third-party claim is brought against them, as a result of the use, misuse or failure to use the CSPs' services. According to the present analysis, only two providers opted not to include such terms in their ToS;[273] which means that such clauses are not only included in paid services, but also in free services, likely affecting billions of users worldwide.

4.3.4 SLAs and Service Credits

A Service Level Agreement (SLA) is a common element in IT contracts, which will aim to define the required level/standard for the services being provided, including one or several ele-

[268] Only 4 surveyed ToS did not indicate a maximum cap for own liability: Basecamp, iCloud (Apple), Microsoft OneDrive and PayPal.
[269] 500px, Facebook and Instagram.
[270] Such is communicated clearly in the ToS for Google Drive which states that its total liability "is limited to the amount you paid us to use the services (or, if the subject of the claim is the free service, to supplying you the services again)"; although such limitation does not exclude/limit any liability that cannot be excluded by law.
[271] See Dropbox ToS.
[272] See Annex I, line b) and q) UCTD.
[273] See Basecamp and Microsoft.

ments – usually called Service Level Objectives (SLO). Each element should be objectively and reliably measurable and binding for the parties, as well as realistic and relevant in the overall scope of the associated contract/services. Such elements will then be "tied" to either a bonus or a penalty/service credit scheme, which will reward or penalise the provider for achieving or failing to achieve those objectives.

In view of this analysis, it was surprising that only one-quarter of the surveyed services provided for an SLA, varying significantly in terms of complexity, length and applicability. Also, most of the services providing SLAs related to one single element, which if not achieved would result in the provision of a service credit to the benefit of the user.[274] Less than half of the services including an SLA establish more complex SLAs with several elements, such as uptime, persistent storage, network performance, support response time and physical security. In this case, additional SLAs would be added if users added additional features to their services.

[274] E.g. Basecamp guarantees a monthly uptime of 99,99%, after which they indicate that they will provide a service credit for the next billing cycle. Additionally, if, in any given day, there is an outage exceeding 5 minutes, Basecamp will credit the user account with an amount equal to ten times the hourly rate that such user pays to use the service.

PART 5 – CONCLUSIONS

The regulatory framework affecting the cloud is complex and very fragmented, a notion which might explain why some authors voice concerns regarding the multiplication (and potential overlaps) of various applicable legislative and those being discussed.[275] At the same time, the existence of a still inherently unbalanced consumer-CSP contractual relationship creates the conditions for a "perfect storm", where CSPs may be forced to comply with unexpected and foreign legal frameworks, while attempting to refuse responsibility towards EU consumers, may hamper customer's confidence and hence decrease the uptake of cloud services.

In parallel, this analysis undertaken demonstrates that the standard agreements for cloud services are far from user-friendly, providing users with few rights and leaving them exposed to data loss and potential liability. In stark contrast, CSPs will be able to (i) terminate the service without cause, (ii) to introduce unilateral changes to the ToS, (iii) to disclaim any type of guarantees and (iv) to exclude direct and indirect liability; these terms are usually accepted by most users either due to ignorance of those or due to the recognition that they do not have sufficient bargaining power to ensure alterations at a reasonable price. As it has been noted above, most clauses will not be valid under EU consumer protection legislation, which may contribute to a wider adoption by consumers; however, SMEs and persons not availing from consumer protection legislation still lack the power to negotiate contractual terms and will be likely forced to accept them, in order to be able to compete in the digital economy market. As such, a measure promoting fair and transparent contractual terms between large cloud integrators and SMEs is also necessary to ensure that the cloud market is not taken hostage by those large players.

Nonetheless, it must be noted that the regulatory background has been evolving and provides an overall positive basis, which promotes security of personal data, increases accountability and ensures more transparency towards users. However, some relevant issues require further analysis and progress, namely those concerning data portability/interoperability and vendor lock-in avoidance. Such areas are of particular importance, since improvements in those can undeniably would contribute to higher levels of competition in the cloud market and put to rest users' fears relating to single-supplier dependence.

---

[275] See Sluijs, Jasper, Larouche, Pierr, Sauter, Wolf, "Cloud Computing in the EU Policy Sphere: Interoperability, Vertical Integration and the Internal Market", 3 JIPITEC 12,2012, paras 84 et seq; see also Balboni, Paolo and Partesott, Claudio, in "Digital Rights Management in the Cloud", in Cloud Computing and Digital Media – Fundamentals, Techniques, and Applications, ed. Li, Kuan-Ching, et all, CRC Press, 2014, pp. 352-356;.see also, section 3.3

In this sense, it is worth highlighting that, following COM (2012)529, industry and public entities have joined efforts with the aim of creating safe and fair contract terms and conditions,[276] as well as to introduce voluntary standards on interoperability, data portability and reversibility,[277] to establish a code of conduct on data protection rules for CSPs[278] and to institute voluntary certification schemes and provide a list of those.[279] Even though some fear that the development of European standards – instead of international ones – could isolate Europe and hamper innovation and competitiveness,[280] others consider that the commitment to such steps will reduce fragmentation within the EU and may serve as a way to encourage the move to the cloud by European businesses and governments. [281]

In 2016, the Commission reaffirmed the importance of ICT standardisation in COM (2016)176.[282] Concerning cloud computing specifically, the Commission indicated that it intended to: (i) improve further interoperability and portability of the cloud (e.g. through the use of open source elements); (ii) facilitate the adoption of cloud computing services by supporting the finalisation of international standards; and (iii) request European Standard Organisations (ESOs) "to update the mapping of cloud standards and guidelines for end users (especially SMEs and the public sector), in collaboration with international SDOs, cloud providers and end users, by mid-2017", thereby ensuring that standards are maintained in line with the global practices. [283] Similarly, Member States have also accompanied the concerns of users and addressed industry, resulting

[276] See "Cloud Service Level Agreement Standardisation Guidelines", Cloud Select Industry Group SLA, 2014: https://ec.europa.eu/digital-single-market/cloud-select-industry-group-service-level-agreements (last accessed 26/04/2020).
[277] In December 2012, the European Commission and the European Telecommunications Standards Institute (ETSI) launched the Cloud Standardization Coordination (CSC) initiative, which has provided a first report in December 2013 – "Cloud Standards Coordination Final Report"), as well four other reports in January 2016 to address issues left open; these documents can be accessed at: http://csc.etsi.org/ (last accessed 17/04/2020).
[278] Two Codes of Conduct (CoC) where presented, one on Data Protection for Cloud Service Providers (June 2016) and another for Cloud Infrastructure Service Providers (latest draft, May 2016). Please note that A29WP provided an opinion on a first draft of the CoC on data protection for Cloud Service Providers, complimenting the effort and suggesting alterations, which were included in the version published on June 2016. Those two documents can be accessed here: https://ec.europa.eu/digital-single-market/en/news/cloud-select-industry-group-csig-plenary-meeting.
[279] See note 253.
[280] See http://www.openforumeurope.org/open-standards-%c2%ad-key-success-delivery-dsm/ (last accessed on 26/04/2020).
[281] See https://www.businesseurope.eu/publications/eu-industrial-digitalisation-strategy-just-time-act-now (last accessed on 26/04/2020).
[282] See COM(2016) 176 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, ICT Standardisation Priorities for the Digital Single Market.
[283] Idem.

in targeted actions which had positive outcomes and may contribute decisively to an increase in the use of cloud computing services.[284]

In this context, and bearing in mind the entire analysis given in this thesis, we are encouraged by the adoption of codes, certification schemes and guidelines, which were discussed by all relevant stakeholders.[285] Furthermore, the adoption of the GDPR, as well as the renovation of the ePrivacy and consumer protection framework, will guarantee the development of the necessary tools to maintain the EU in the foreground of the data-driven economy, by providing safe and reliable marketplaces and online services. On the other hand, legislators (at EU and national level) should resist the temptation of over-regulating the sector, given that such may also stifle innovation and competitiveness of the European CSPs.

In addition to legislation, it should be noted that the use of soft law and co-regulatory instruments is also in line with the current preferred practice suggested by various scholars[286] and businesses[287], given its ability to adjust to the constant evolution of this area. Such approach provides the flexibility required when dealing with technology, while allowing industry and policy makers to more easily adjust previous commitments to unpredictable situations, without requiring a burdensome legislative process, which by the time is adopted may no longer be relevant. Additionally, parallel initiatives, supported by different stakeholders, have been providing also further information and transparency (such as SLALOM[288], ToS;DR[289], tl;drLegal[290]), contributing to both clearer and fairer terms, as well as to a better understanding of the underlying conditions of accepting some information society services. As Millard noted, at given that the main obstacle to the further adoption of cloud services results from a mismatch of starting assumptions, it is up to CSPs not only to "to provide the advantages of the cloud to consumers", but also to convey "an adequate understanding of the nature and risks of the service, and [thereby] achieving a fair and reasonable allocation of the risks involved".[291]

---

[284] See https://www.gov.uk/government/news/cma-secures-better-deal-for-cloud-storage-users, last accessed on 26/04/2020.
[285] See https://news.microsoft.com/cloudforgood/spotlight/soft-law-benefits-standards.html.
[286] See McGillivray (op. cit. in note 199), p.24-25, and Millard, et. al (op. cit. in note 27), p. 344-346 and 383-384.
[287] Note 285.
[288] SLALOM is a project co-funded by the Commission through the Horizon2020 Programme which provides legal model clauses, technical specifications for SLAs and guidance models on how to apply them For more information please see http://slalom-project.eu/.
[289] ToS; DR stands for "Terms of Service; Didn't Read" which is a "user rights initiative to rate and label website for terms & privacy policies", which are rated from very good (Class A) to very bad (Class E)". For more information please see https://tosdr.org/.
[290] tl;drLegal is website which relies on a community (and also on lawyers/experts) to provide simple and practical summaries of ToS and Licence terms. For more information please see https://tldrlegal.com/.
[291] See Millard, et. al (op. cit. in note 27), p. 361

Besides the implementation (and compliance by the CSPs) of the aforementioned legislation, I consider that the adoption of clearer and fairer contractual terms, as well as the introduction of standards/mechanisms enforcing data portability and system interoperability, will represent a definite step to ensure a more balanced relationship between users (namely those not able to negotiate specific contractual terms – i.e. consumers, SMEs, individual professionals) and CSPs. Specifically, I have confidence that, by granting users the possibility of exchanging CSPs with little difficulty, CSPs may be more inclined to hear the requests of smaller users, either those relate to undertaking higher degrees of security, providing better service continuity, or committing to data integrity. In addition to that, the widespread access to information on the quality/risks associated to certain services, will certainly contribute to the creation of more prepared and engaged cloud computing users and to choosing CSPs, which promote more balanced relationships with their clients. Ultimately, CSPs which will be quicker to react to user's feedback, to tackle their concerns and adapt to the requests for data security and privacy, will enjoy a better public image and likely see an increase in their customer base.

BIBLIOGRAPHY

BOOKS AND ARTICLES

BLOKDIJK, Gerard - Service Level Agreement 100 Success Secrets. [S.l.] : Emereo Publishing, 2008.

BRADSHAW, David *et al.* - Uptake of Cloud in Europe - Follow-up of IDC study on quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up. Digital Agenda for Europe. 2014.

BRADSHAW, Simon; MILLARD, Christopher; WALDEN, Ian - Contracts for clouds: A comparative analysis of terms and conditions for cloud computing services. Queen Mary School of Law Legal Studies Research Paper. 63:2010.

BRADSHAW, Simon; MILLARD, Christopher; WALDEN, Ian - Standard contracts for cloud services. Cloud Computing Law. 2013, 39–72.

BUCILLA, James R. - The Online Crossroads of Website Terms of Service Agreements and Consumer Protection: An Empirical Study of Arbitration Clauses in the Terms of Service Agreements for the Top 100 Websites Viewed in the United States. Wake Forest Journal of Business and Intellectual Property Law. 15:2014, 102–148.

BURNETT, Rachel - Outsourcing IT: the legal aspects. 2nd. ed. [S.l.] : Gower Publishing, Ltd., 2009. ISBN 0-566-07698-5.

BURNETT, Rachel; KLINGER, Paul - Drafting and negotiating computer contracts. 2nd. ed. [S.l.] : Tottel Publishing, 2005. ISBN 1-84592-000-7.

BUYYA, Rajkumar; BROBERG, James; GOSCINSKI, Andrzej M. - Cloud computing: Principles and paradigms, John Wiley & Sons, 2010. ISBN 1-118-00220-2.

BYGRAVE, Lee A. - Privacy protection in a global context–a comparative overview. Scandinavian Studies in Law. 47:2004, 319–348.

COLES, Cameron *et al.* - Cloud adoption practices & priorities survey report. Cloud Security Alliance. 2015.

CUNNINGHAM, Alan; REED, Chris - Caveat Consumer?– Consumer Protection and Cloud Computing Part 2 –The Application of ex ante and ex post Consumer Protection Law in the Cloud. Queen Mary School of Law Legal Studies Research Paper No. 133/2013. 2013.

CUNNINGHAM, Alan; REED, Chris - Caveat Consumer?–Consumer Protection and Cloud Computing Part 1 – Issues of Definition in the Cloud. Queen Mary School of Law Legal Studies Research Paper No. 130/2013. 2013)

DE HERT, Paul; GUTWIRTH, Serge - Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. in CLAES, ERIK; DUFF, ANTONY; GUTWIRTH, SERGE (Eds.) - Privacy and the criminal law. [S.l.] : Intersentia, 2006. p. 61–104.

DE HERT, Paul; GUTWIRTH, Serge - Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. Privacy and the criminal law. 2006) 61–104.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis; KAMARA, Irene - The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection. Computer Law & Security Review. . ISSN 0267-3649. 32:1 (2016) 16–30.

ETRO, Federico - The Economics of Cloud Computing. IUP Journal of Managerial Economics. . ISSN 0972-9305. 9:2 (2011).

FARBER, Dan - Oracle's Ellison nails cloud computing. [Em linha] (26 set. 2008). . Disponível em WWW:<URL:https://www.cnet.com/news/oracles-ellison-nails-cloud-computing/>.

FINCK, Michèle; PALLAS, Frank - They Who Must Not Be Identified-Distinguishing Personal from Non-Personal Data Under the GDPR. Max Planck Institute for Innovation & Competition Research Paper. 19–14 (2019).

FINCK, Michèle; PALLAS, Frank - They Who Must Not Be Identified-Distinguishing Personal from Non-Personal Data Under the GDPR. Max Planck Institute for Innovation & Competition Research Paper. 19–14 (2019).

FOSTER, Ian; KESSELMAN, Carl (EDS.) - The Grid 2: Blueprint for a new computing infrastructure. 2nd. ed. [S.l.] : Elsevier, 2003. ISBN 0-08-052153-3.

GEELAN, Jeremy - Twenty one experts define cloud computing. Virtualization. August 2008. Electronic Magazine. 2009).

GUTWIRTH, Serge *et al.* - Reinventing data protection? [S.l.] : Springer, 2009. ISBN 1-4020-9498-1.

Handbook on European data protection law - . [S.l.] : European Union Agency for Fundamental Rights and Council of Europe, 2018

HON, Kuan W.; HÖRNLE, Julia; MILLARD, Christopher - Which law (s) apply to personal data in clouds. Em Cloud Computing Law. [S.l.] : Oxford University Press Oxford, 2013. p. 220–248.

HON, W. Kuan; MILLARD, Christopher; WALDEN, Ian - The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing. International Data Privacy Law. . ISSN 2044-4001. 1:4 (2011) 211–228.

HON, W. Kuan; MILLARD, Christopher; WALDEN, Ian - Who is responsible for 'personal data'in cloud computing?—The cloud of unknowing, Part 2. International Data Privacy Law. . ISSN 2044-4001. 2:1 (2012) 3–18.

JOHNSON, Bobby - Cloud computing is a trap, warns GNU founder Richard Stallman. The Guardian. [Em linha] (29 set. 2008). . Disponível em WWW:<URL:https://www.theguardian.com/technology/2008/sep/29/cloud.computing.richard.stallman>.

LANOIS, Paul - Caught in the clouds: The Web 2.0, cloud computing, and privacy. Northwestern Journal of Technology and Intellectual Property. 9:2010) 29.

LI, Kuan-Ching; LI, Qing; SHIH, Timothy K. - Cloud computing and digital media: fundamentals, techniques, and applications. [S.l.] : CRC press, 2014. ISBN 0-429-09964-9.

MCGILLIVRAY, Kevin - A right too far? Requiring cloud service providers to deliver adequate data security to consumers. International Journal of Law and Information Technology. . ISSN 0967-0769. 25:1 (2017) 1–25.

MELL, Peter; GRANCE, Tim - The NIST definition of cloud computing. 2011).

MILLARD, Christopher J. - Cloud computing law. [S.l.] : Oxford University Press Oxford, 2013. ISBN 0-19-967168-0.

MOEREL, Lokke - The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? International Data Privacy Law. . ISSN 2044-4001. 1:1 (2011) 28–46.

MOEREL, Lokke - Binding corporate rules: corporate self-regulation of global data transfers. [S.l.] : OUP Oxford, 2012. ISBN 0-19-163996-6.

POTHOS, Mary - Accountability Requirements. Em USTARAN, EDUARDO (Ed.) - European Data Protection: Law and Practice. [S.l.] : IAPP, 2018. p. 193–211.

RITTINGHOUSE, John W.; RANSOME, James F. - Cloud computing: implementation, management, and security. [S.l.] : CRC press, 2010. ISBN 1-4398-0681-0.

RUDGARD, Sian - Origins and historical context of data protection law. Em USTARAN, EDUARDO (Ed.) - European Data Protection: Law and Practice. [S.l.] : IAPP, 2018

SLUIJS, Jasper P.; LAROUCHE, Pierre; SAUTER, Wolf - Cloud computing in the EU Policy Sphere: Interoperability, vertical integration and the internal market. J. Intell. Prop. Info. Tech. & Elec. Com. L. 3:2012) 12.

SPINDLER, Gerald; SCHMECHEL, Philipp - Personal data and encryption in the European general data protection regulation. JIPITEC. 7:2016) 163.

VAN ALSENOY, Brendan - The Evolving Role of the Individual Under EU Data Protection Law. CiTiP Working Paper 23/2015. 2015).

WEINMAN, Joe - Cloudonomics: The business value of cloud computing. [S.l.] : John Wiley & Sons, 2012. ISBN 1-118-28288-4.

WENDEHORST, Christiane - Platform intermediary services and duties under the e-commerce directive and the consumer rights directive. Journal of European Consumer and Market Law. . ISSN 2364-4710. 5:1 (2016) 30–33.

LEGISLATION:

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data. (85-10-01)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, revised by Directive (EU)2015/2302 of the European Parliament and of the Council of 25 November 2015 and Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194/1, 19.7.2016.

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM (2017) 10 final.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

REPORTS, WORKING DOCUMENTS, RECOMMENDATIONS:

ARTICLE 29 WORKING PARTY - Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (Report n. WP 56).

ARTICLE 29 WORKING PARTY - Opinion 4/2007 on the concept of personal data (Report n. WP136).

ARTICLE 29 WORKING PARTY - Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (Report n. WP 133).

ARTICLE 29 WORKING PARTY - Working Document setting up a framework for the structure of Binding Corporate Rules (Report n. WP 154).

ARTICLE 29 WORKING PARTY - Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (Report n. WP 153).

ARTICLE 29 WORKING PARTY - The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data: European Commission, 2009 (Report n. WP168).

ARTICLE 29 WORKING PARTY - Opinion 1/2010 on the concepts of "controller" and "processor" (Report n. WP169).

ARTICLE 29 WORKING PARTY - Opinion 8/2010 on applicable law (Report n. WP179).

ARTICLE 29 WORKING PARTY - Opinion 15/2011 on the definition of consent (Report n. WP187).

ARTICLE 29 WORKING PARTY - Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities (Report n. WP 195a).

ARTICLE 29 WORKING PARTY - Opinion 05/2014 on Anonymisation Techniques (Report n. WP216).

ARTICLE 29 WORKING PARTY - Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (Report n. WP217).

ARTICLE 29 WORKING PARTY - Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on "Contractual clauses" considered as compliant with the EC Model Clauses (Report n. WP 226).

ARTICLE 29 WORKING PARTY - Opinion 8/2010 on applicable law (update) (Report n. WP179-update).

ARTICLE 29 WORKING PARTY - Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, WP238, 2016 (Report n. WP 238).

BEUC - BEUC contribution to the European Commission's Expert Group on Cloud Computing Contracts - Unfair Contract Terms in Cloud Computing Service Contracts Discussion Paper, [Online] Available at: http://www.beuc.eu/publications/beuc-x-2014-034_are_ec_expert_group_on_cloud_computing_contracts.pdf.

COMPETITION & MARKETS AUTHORITY - Consumer law compliance review: cloud storage – findings report [Online] Available at :https://assets.digital.cabinet-office.gov.uk/media/57472953e5274a037500000d/cloud-storage-findings-report.pdf.

COUNCIL OF EUROPE - Recommendation No. (2006) 4 of the Committee of Ministers to Member States on research on biological materials of human origin. 2006.

EUROPEAN COMMISSION - COM(2012) 529 final, Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions.

EUROPEAN DATA PROTECTION BOARD - Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

EUROPEAN DATA PROTECTION BOARD - Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects.

EUROPEAN DATA PROTECTION BOARD - Guidelines 05/2020 on consent under Regulation 2016/67.

European Commission's «New Deal For Consumers», COM (2018) 183.

European Parliament resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP)).

EUROSTAT - Cloud computing - statistics on the use by enterprises [Online], Dec. 2018. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises#Cloud_computing_as_a_service_model_for_meeting_enterprises.E2.80.99_ICT_needs.

Report from the Commission to the European Parliament and the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield, COM (2018) 860 final, 2018.

Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield, COM (2019) 495 final, 2019.

Staff Working Document. accompanying the Report from the Commission to the European Parliament and the Council on the Third Annual Review of the Functioning of the EU-U.S. Privacy Shield, SWD (2019) 390 final, 2019.

ANNEX I –OVERVIEW OF TERMS OF SERVICE

I. Section 4.1.1 – Duration and Consideration

	Duration	Consideration
500px	Open-end, as per ToS (section Termination): "If you wish to terminate your 500px account, you may simply discontinue using the Services."	Includes both free and paid (premium) accounts; in addition, users grant 500px a non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, distribute, reproduce, modify, adapt, publicly perform and publicly display Content provided by the User and for the period during which the content is posted on 500px.
AWS	Open-end, as per Section. 7.1 of the Customer Agreement: "The term of this Agreement will commence on the Effective Date and will remain in effect until terminated under this Section 7."	Monthly payments for the selected services.
ADRIVE	Open-end and extended on a monthly or yearly basis, as per Section B.1, (ii): "You may cancel Your Paid Account by notifying ADrive at billing@adrive.com of Your desire to terminate and Your account will be terminated effective at the end of the current subscription period."	Free and paid versions, depending on plan; in addition, Users grant a non-exclusive, sub-licensable license to ADrive for any and all rights in the identifications, descriptions, or other metadata you have provided in connection with your Storage Data. ADrive reserves the right to rent, sell or otherwise share this metadata with other entities at its discretion.
Basecamp	Open-end, as per ToS (section Cancellation and Termination): "You can cancel your account at any time by clicking on the Account link in the global navigation bar at the top of the screen. The Account screen provides a simple no-questions-asked cancellation link."	Free and paid versions.
Datapipe	Fixed term with automatic extension, unless otherwise opposed by either Party, as per section 7.1 of ToS: "This Agreement will continue until the end of the term set forth in Customer's Account, or until the end of the current calendar month if Customer's Account does not list a term (collectively, the "Term"). At the end of each Term, this Agreement will renew for an additional Term of the same duration, unless either party gives written notice of its intent not to renew 30 or more days before the end of the current Term."	Pay-as-You-Go plans or Prepaid plans (overage fees may be applicable).
Dropbox	For free accounts, the account will be terminated if the User hasn't accessed Services for 12 consecutive months; for paid accounts, the duration is set forth on the Order Form.	Free and paid accounts
Facebook	Users may "account or disable (…) application at any time." Accounts of deceased users may be memorialised[292]	Free service; users grant Facebook "a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it."
Google	Open-end, as per ToS (section Modifying and Terminating our Ser-	Free (up to 15GB) and paid accounts; Google Drive Users "give Google a worldwide license to use,

[292] https://www.facebook.com/help/1506822589577997/

Drive	vices): "You can stop using Google Drive at any time, although we'll be sorry to see you go. We may suspend or permanently disable your access to Google Drive"	host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our services, and to develop new ones. This license continues even if you stop using our services unless you delete your content. Make sure you have the necessary rights to grant us this license for any content that you submit to Google Drive."
iCloud	Open-end, as per section VII A. of ToS (UK): "You may delete your Apple ID and/or stop using the Service at any time." In addition "Apple may at any time, under certain circumstances and without prior notice, immediately terminate or suspend all or a portion of your Account and/or access to the Service." (see section VII B. of ToS (UK)).	Free and Paid accounts "Except for material we may license to you, Apple does not claim ownership of the materials and/or Content you submit or make available on the Service. However, by submitting or posting such Content on areas of the Service that are accessible by the public or other users with whom you consent to share such Content, you grant Apple a worldwide, royalty-free, non-exclusive license to use, distribute, reproduce, modify, adapt, publish, translate, publicly perform and publicly display such Content on the Service solely for the purpose for which such Content was submitted or made available, without any compensation or obligation to you.
Instagram	Open-end, as per ToS (General Conditions, section 1): "We reserve the right to modify or terminate the Service or your access to the Service for any reason, without notice, at any time, and without liability to you. You can deactivate your Instagram account by logging into the Service"	Free service; users "grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service"
Linode	Open-end, as per ToS: "You may cancel the service at any time by using the "Cancel Account" link" and "Linode.com reserves the right to suspend network access to any customer if, in the judgment of the Linode.com network administrators, the customer's server is the source or target of a violation of any of the other terms of service or for any other reason which Linode.com chooses."	Paid services
MEGA	Open-end, as per ToS: "You can terminate your access to the website and our services at any time" and "We may also terminate or suspend our services or any part of our services, for all users or for groups of users, without notice, at any time, for any reason or no reason."	Free and paid services
Microsoft OneDrive	Open-end, as per ToS:"we reserve the right to close your account and delete or disable access to Your Content on OneDrive" and "you can cancel specific Services or close your Microsoft account or Skype account at any time and for any reason (…) When you ask us to close your Microsoft account, we will put it in a suspended state for 60 days just in case you change your mind."	Free and Paid services; in addition users "grant Microsoft a worldwide and royalty free intellectual property licence to use Your Content, for example, to make copies of, retain, transmit, reformat, distribute via communication tools and display Your Content on the Services. If you publish Your Content in areas of the Service where it is rendered available online publicly or without restrictions, Your Content may appear in demonstrations or materials that promote the Service."
Norton Online Backup	Fixed term, as per ToS "The "Service Period" (…) shall continue for the period of time set forth in the Service documentation or the applicable transaction documentation from the authorized distributor or reseller from which You obtained the Software or Service."	Paid services

PayPal	Open-end, as per ToS: "This Agreement starts when you successfully register for a PayPal account and ends when your Account is closed for whatever reason, except that this Agreement survives termination to the extent and for so long as we require to deal with the closure of your Account and to comply with applicable laws and regulations"	A payment is required from either the sender or the recipient of monies; additionally, users grant Paypal the following rights of use: "Your business-related intellectual property: You grant the PayPal Group the worldwide right to use and depict your business name, trademarks and logos on our website and in our mobile and web applications for the purpose of displaying information about your business and its products and services. (…) Your content: When providing us with content or posting content (in each case for publication, whether on- or off-line) using the Services, you grant the PayPal Group a non-exclusive, worldwide, perpetual, irrevocable, royalty-free, sublicensable (through multiple tiers) right to exercise any and all copyright, publicity, trademarks, database rights and intellectual property rights you have in the content, in any media known now or in the future."

II. Section 4.1.2 – Applicable Law and Jurisdiction

	Applicable Law	**Jurisdiction**
500px	USA, State of New York	New York, New York; San Francisco, California
AWS	USA, State of Washington.	(mandatory arbitration – no jurisdiction specified)
ADRIVE	USA, State of California	San Francisco, California (Arbitration)
Basecamp	Matter is not defined in the ToS; no reply was provided on this matter following email exchanges with Basecamp.	Matter is not defined in the ToS; according to email exchanges with Basecamp "our jurisdiction is the place where Basecamp has its central administration and/or servers, which in our case are all in the US."
Datapipe	USA, State of California	San Francisco, California
Dropbox	USA, California, except in countries "with laws that give consumers the right to bring disputes in their local courts" (e.g. EU Consumers).	USA, California, San Francisco, except in countries that "have laws that require agreements to be governed by the local laws of the consumer's country", e.g. EU Consumers); but Dropbox requests users to attempt to try to informally resolve disputes by contacting dispute-notice@dropbox.com.
Facebook	USA, State of California	U.S. District Court for the Northern District of California or a state court located in San Mateo County
Google Drive	"If you live outside the European Union, the laws of California, U.S.A" and "If you live in the European Union, the laws and courts of your country of residence will apply to any disputes arising out of or relating to these Terms or Google Drive..."	"All claims arising out of or relating to these Terms or Google Drive will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts." If living in the EU, then the users' local courts and "Disputes may be submitted for online resolution to the European Commission Online Dispute Resolution platform."
iCloud	USA, State of California, unless "you are a citizen of any European Union country or Switzerland, Norway or Iceland, [then] the governing law and forum shall be the laws and courts of your usual place of residence."	County of Santa Clara, California, unless "you are a citizen of any European Union country or Switzerland, Norway or Iceland, [then] the governing law and forum shall be the laws and courts of your usual place of residence."
Instagram	USA, State of California;	State or federal court located in Santa Clara, California, and to submit to the personal jurisdiction of the courts located in Santa Clara County for the purpose of litigating all such disputes.

Linode	USA, State of New Jersey	Courts located within the county of Atlantic, New Jersey, USA.
MEGA	New Zealand law	New Zealand arbitral tribunals (and courts for the purposes of that enforcement of any arbitral award or appeal on question of law)
Microsoft OneDrive	"If you live in (or, if you are a business, your principal place of business is in) Europe and you are using cost-free portions of the Services (…)[t]he laws of Washington State, USA govern all claims related to cost-free Services, without prejudice to the mandatory law provisions which apply in the country to which we direct your Services where you have your habitual residence."(…)"If you have paid to use a portion of the Services (...)[t]he laws of the country to which we direct your Services where you have your habitual residence govern all claims relating to paid Services."	"With respect to jurisdiction, you and Microsoft agree to choose the courts of the country to which we direct your Services where you have your habitual residence for all disputes arising out of or relating to these Terms, or in the alternative, you may choose the responsible court in Ireland."
Norton Online Backup	State of California, USA	State or federal court in Santa Clara County, California
PayPal	"Agreement and the relationship between us shall be governed by English law, subject to your local mandatory rights."	"For complaints that cannot be resolved otherwise, you submit to the non-exclusive jurisdiction of the English courts arising out of or relating to this Agreement or the provision of our Services without prejudice to your right to also initiate a proceeding against PayPal in that context before the competent courts of and in Luxembourg.

III. Section 4.1.3 – Acceptable Use Polices

Acceptable Use Policies (AUP)

500px	"As a condition of use, you promise not to use the Services for any purpose that is unlawful or prohibited by these Terms, or any other purpose not reasonably intended by 500px." (…) "500px maintains a fair storage policy to ensure stable and fast service to all users."
AWS	AWS AUP - includes: illegal, harmful and fraudulent activities; infringing content (IPR), offensive or harmful content; security violations, network abuse email/message abuse (i.e. spam).
ADRIVE	"You shall not use the ADrive Services to transmit, transfer or convey Storage Data that might be illegal or otherwise damaging to ADrive, its users, or others…."; includes typical provisions on IPR infringement, defamatory, unlawful, harassing content, harmful, illegal uses, viruses…
Basecamp	A clear AUP is not included, but standard limitations are included, such as: "You may not use the Service for any illegal purpose or to violate any laws in your jurisdiction (including but not limited to copyright laws)."and "Verbal, physical, written or other abuse (including threats of abuse or retribution) of any Service customer, Company employee or officer will result in immediate account termination." (…) We reserve the right to temporarily disable your account if your usage significantly exceeds the average usage of other Service customers."
Datapipe	Includes a dedicated AUP, covering Spam; IPR infringement; hacking; dissemination of offensive info (threatening, libellous, obscene or harassing); child pornography; Fraud; violation of privacy , publicity, trade secret rights; virus distribution; use/host of an IRC server. Datapipe may suspend services if it reasonably suspects an AUP violation.
Dropbox	Yes (typical clause) – probe/scan for system's vulnerabilities: breach/circumvent authentication measures; interfere with the Services; spam/spoofing, phishing; publish/share materials that are unlawfully pornographic or indecent, or that contain extreme acts of violence; advocate bigotry or hatred; violate the law; violate the privacy/rights of others.

Facebook	Yes (see sections 3-5 ToS, under the headings "Safety", "Registration and Account Security" and "Protecting Other People's Rights").
Google Drive	"We may review content to determine whether it is illegal or violates our Program Policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do." The "Program Policies" abuses of the service include: spam; violence; hate speech, harassment, bullying and threats; sexually explicit material (writing about adult topics is permitted); child exploitation; impersonation; sharing of personal and confidential info; illegal activities; copyright infringement; "By accepting these terms, you agree not to use Google Drive for business purposes; you must use the Drive service only for personal non-commercial purposes."
iCloud	Yes, included as "B. Your Conduct", in the ToS; it cover the following: (i) making available Content that is unlawful, harassing, threatening, harmful, tortious, defamatory, libelous, abusive, violent, obscene, vulgar, invasive of another's privacy, hateful, racially or ethnically offensive, or otherwise objectionable; (ii) stalk, harass, threaten or harm; (iii) request personal information from a minor not personally known to the user; (iv) pretend to be another person/entity; copyright/IPR infringement; spam, junk mail; forge TCP-IP packet header; make available viruses / code made to harm/interfere with the Service or any SW/HW; interfere with Service or servers/network; plan/engage in illegal activities; gather personal info of users of the Service in connection with prohibited activities.
Instagram	Yes, in Chapter "Basic Terms", point 2, 6-7, 9-16, including not posting "violent, nude, partially nude, discriminatory, unlawful, infringing, hateful, pornographic or sexually suggestive photos"; not defame, stalk, bully, abuse, harass, threaten, impersonate or intimidate; use service for any illegal/unauthorised purpose; not change, modify, adapt or alter the Service; not to spam; not to use domain names or web URLs; not interfere/disrupt service; comply with Instagram's Guidelines[293], etc…
Linode	Yes, see section 2&3. User's must abstain from interfering with Linode's services/networks and are prohibited from: misusing system resources; spamming; mailing lists for a targeted audience, allowing removal; accessing other computers/networks without authorisation; providing illegal or harmful activities or false data. Linode allows P2P services (i.e. ToR)
MEGA	Yes, see section 13. Includes: transfer/assign rights to the services; damage, disrupt or burden Mega's website or someone else's website; infringe IPR; resell or supply the services; use/transmit data which violates the law, sending spam; abuse, harass, defame, stalk...; data which is unsuitable, offensive, obscene or discriminatory information; run network scanning SW; upload anything that could interfere with the services, network, device or system; to impersonate someone.
Microsoft OneDrive	Yes, under 3 Code of Conduct, it bars the following: doing anything illegal; engaging in activities that exploit, harm or threaten children; spamming; publicly display or share inappropriate Content or other material (involving, for example, nudity, bestiality, pornography, graphic violence or criminal activity); engaging in false/misleading activities; wilful circumvention of restrictions on access/availability of Services; engaging in activities harmful to self, the services or others (e.g. transmitting viruses, stalking, posting terrorist content, communicating hate speech or advocating violence against others); infringing rights of other; privacy violating activities; helping other breaking the rules
Norton Online Backup	Yes, User Conduct and Responsibility, prohibited uses includes "(i) use the Service for illegal purposes, (ii) transmit or store material that may infringe the intellectual property rights or other rights of third parties or that is illegal, tortious, defamatory, libelous, or invasive of another's privacy; (iii) transmit or store Data belonging to another party without first obtaining all consents required by law from the Data owner for transmission of the Data to Symantec for storage within the United States; (iv) transmit any material that contains software viruses or other harmful computer code, files or programs such as trojan horses, worms or time bombs; (v) interfere with or disrupt servers or networks connected to the Service; or (vi) attempt to gain unauthorized access to the Service, the accounts of other Service users, or computer systems or networks connected to the Service.
PayPal	Yes, own document – AUP incorporated by reference in the Paypal User Agreement. However, this last document also includes a **section on Restricted Activities (9.1)**. The AUP includes typical prohibited activities/transactions (relating to illegal activities, promotion of hate/violence, obscene items, infringing IPR or privacy rights, etc.), and also bans those relating to sexually oriented materials/services and firearms and ammunition and weapons/knives when regulated under the applicable law). In addition, Paypal's AUP indicates that some activities require pre-approval (I.e. relating to airlines, donations for charities, providing file sharing, selling alcoholic beverages, activities related to gambling/gaming…)

IV. Section 4.1.4 – Termination

[293] https://help.instagram.com/customer/portal/articles/262387-community-guidelines

	Termination
500px	"500px may terminate or suspend any and all Services and/or your 500px account immediately, without prior notice or liability, for any reason whatsoever, including without limitation if you breach the Terms."
AWS	Termination for convenience : 30 days (either party); Termination for uncured material breach: 30 days (either party); Immediate termination by AWS: (i) after a suspension; (ii) if 3rd party stops offering SW or Tech used by the Service; (iii) to comply with law or requests by governmental entities.
ADRIVE	Termination for convenience: by ADrive (right to change/suspend/discontinue aspects of services available); by either Party, for any reason or for no reason by sending notice of termination. Termination for cause (ADrive) for breach of provisions, law violation. In this case, the user will no longer have the right to use the ADrive Services (it is not clear if retrieval of data will be allowed);
Basecamp	Termination by User, immediate by cancellation link. "The Company, in its sole discretion, has the right to suspend or terminate your account and refuse any and all current or future use of the Service for any reason at any time. Such termination of the Service will result in the deactivation or deletion of your Account or your access to your Account, and the forfeiture and relinquishment of all content in your account. The Company reserves the right to refuse service to anyone for any reason at any time."
Datapipe	For material breach (by either party), by written notice, termination effective 30 days after notice; if the breach is subject to cure and the other party cures it, no termination.
Dropbox	The user is "free to stop using (…) Services at any time". – does this equate to termination? Termination by Dropbox, if: user breaches ToS; use of services could cause risk of harm to Dropbox or other users; or user does not have a paid account and has not accessed for 12 consecutive months (usually called delinquency). Dropbox will provide reasonable advance for the user to remedy the situation and export his Stuff (i.e. data, content, files, etc.), unless: the user is in material breach; doing so would cause legal liability to Dropbox/compromise ability to provide Services; Dropbox is prohibited from doing so by law. Also, "We may decide to discontinue the Services in response to unforeseen circumstances beyond Dropbox's control or to comply with a legal requirement. If we do so, we'll give you reasonable prior notice so that you can export Your Stuff from our systems"
Facebook	Termination by Facebook "If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us (…) We will notify you by email or at the next time you attempt to access your account. Termination by user: delete account or disable your application at any time.
Google Drive	"You can stop using Google Drive at any time, although we'll be sorry to see you go. We may suspend or permanently disable your access to Google Drive if you materially or repeatedly violate our Terms or our Program Policies. We will give you prior notice of us suspending or disabling your access to Google Drive. However, we may suspend or disable your access to Google Drive without notice if you are using Google Drive in a manner that could cause us legal liability or disrupt other users' ability to access and use Google Drive." "If we decide to discontinue Google Drive, we will give you at least 60 days' prior notice. During this notice period, you will have the opportunity to take your files out of Google Drive. After the end of this 60 day period you will not be able to access your files."
iCloud	Termination by User – delete Apple ID or request termination, via Apple Support. Termination by Apple – "at any time, under certain circumstances and without prior notice, immediately terminate or suspend all or a portion of your Account and/or access to the Service. Cause for such termination shall include: (a) violations of this Agreement (…); (b) a request by you to cancel or terminate your Account; (c) a request and/or order from law enforcement, a judicial body, or other government agency; (d) where provision of the Service to you is or may become unlawful; (e) unexpected technical or security issues or problems; (f) your participation in fraudulent or illegal activities; or (g) failure to pay any fees owed by you (…) in relation to the Service, provided that in the case of non-material breach, Apple will be permitted to terminate only after giving you 30 days' notice and only if you have not cured the breach within such 30-day period. Any such termination or suspension shall be made by Apple in its sole discretion and Apple will not be responsible to you or any third party for any damages that may result or arise out of such termination or suspension of your Account and/or access to the Service. Termination by delinquency – "Apple may terminate your Account upon 30 days' prior notice (…) if (a) your Account has been inactive for one (1) year;" Discontinuation of service – "Apple may terminate your Account upon 30 days' prior notice via email to the address associated with your Account if (…) (b) there is a general

	discontinuance of the Service or any part thereof." Effects of Termination – Users "may lose all access to the Service and any portions thereof, including, but not limited to, your Account, Apple ID, email account, and Content. In addition, after a period of time, Apple will delete information and data stored in or as a part of your account(s)."
Instagram	"Violation of these Terms of Use may, in Instagram's sole discretion, result in termination of your Instagram account." "We reserve the right to modify or terminate the Service or your access to the Service for any reason, without notice, at any time, and without liability to you. You can deactivate your Instagram account by logging into the Service and completing the form available here: https://instagram.com/accounts/remove/request/. If we terminate your access to the Service or you use the form detailed above to deactivate your account, your photos, comments, likes, friendships, and all other data will no longer be accessible through your account (e.g., users will not be able to navigate to your username and view your photos), but those materials and data may persist and appear within the Service (e.g., if your Content has been re-shared by others).
Linode	Termination with cause: "Linode.com reserves the right to suspend network access to any customer if, in the judgment of the Linode.com network administrators, the customer's server is the source or target of a violation of any of the other terms of service or for any other reason which Linode.com chooses. Linode.com will use reasonable care in notifying the Customer and in resolving the problem in a method resulting in the least amount of service interference. Linode.com reserves the right to terminate service without notice for continued and repeated violations of the terms of service. If inappropriate activity is detected, all accounts of the Customer in question will be deactivated until an investigation is complete. Prior notification to the Customer is not assured. In extreme cases, law enforcement will be contacted regarding the activity. The customer will not be credited for the time the customer's machines were suspended. Termination without cause – "If at any time it becomes necessary for Linode.com to cancel a customer's service without cause, Linode.com will provide 30 days advance notice."; User Termination – "You may cancel the service at any time by using the "Cancel Account" link located on the "My Accounts" sub-tab of the Linode Manager. Accounts are cancelled immediately after confirmation. Cancellation of service does not relieve Subscriber of responsibility for the payment of all accrued charges." Termination following request for disclosure by law enforcement – "In addition, Linode.com shall have the right to terminate all service set forth in this Agreement." Termination resulting from prohibited usage: - "You agree that any of the below activities are considered prohibited usage and will result in immediate account suspension or cancellation without a refund and the possibility that Linode.com will impose fees; and/or pursue civil remedies without providing advance notice."
MEGA	User Termination: "You can terminate your access to the website and our services at any time by sending an email to support@mega.nz requesting termination or by following the 'Cancel your account' link" Mega Termination: "We can immediately suspend or terminate your access to the website and our services without notice to you: 31.1 if you breach any of these terms or any other agreement you have with us; 31.2 if you are not a registered user, at any time; 31.3 if you are using a free account and that account has been inactive for over 3 months or we have been unable to contact you using the email address in your account details. 32 We may also terminate or suspend our services or any part of our services, for all users or for groups of users, without notice, at any time, for any reason or no reason. (see retrieval upon termination)
Microsoft OneDrive	ToS "if you violate any of the obligations listed in section 3(a) above or otherwise materially violate these Terms, we may take action against you including (without limitation) stopping providing Services or closing your Microsoft account or Skype account immediately for good cause or blocking delivery of a communication (like email or instant message) to or from the Services. We also reserve the right to remove or block Your Content from the Services at any time if it is brought to our attention that it may violate applicable law or these Terms. When investigating alleged violations of these Terms, Microsoft reserves the right to review Your Content in order to resolve the issue. However, we do not monitor the Services and make no attempt to do so. OneDrive specific terms: "If you have more content stored in your OneDrive account than is provided to you (…) and you do not respond to notice from Microsoft (…) we reserve the right to close your account and delete or disable access to Your Content on OneDrive." (…) "We will give you at least one month's notice before closing your OneDrive account for inactivity under section 4(a)(ii). If you are a paid OneDrive subscriber, we won't close your account for inactivity during any period where you have paid for your OneDrive usage."
Norton Online Backup	"Your right to use the Service shall terminate upon expiration of the Service Period. In addition, Symantec may, at its sole discretion, immediately suspend or terminate use of the Service during the Service Period for your failure to or Symantec's reasonable belief that you have failed, to comply with these terms and conditions or any other misuse of the Service. Following the expiration or termination of the Service Period: Data stored to the online backup space provided with Your Service will be at risk of being purged; Syman-

	tec shall not be obligated to maintain such Data, forward such Data to You or a third party, or migrate such Data to another backup service or account; and You will not be able to store Data to any additional backup space under the Service that You may have purchased separately unless and until Your current Service Period is renewed or Your new Service Period is activated.
PayPal	By User: "You can close your Account at any time by logging into your Account, clicking on the "Profile" tab, clicking on the "Close Account" link, and then following the instructions."; By Paypal: "We may close your Account at our convenience by providing you with two months' prior notice. We may also close your Account at any time where: (i) you are in breach of the terms of this Agreement and/or we are entitled to close your Account under section 10.2; (ii) you do not access your Account for three years; or (iii) we suspect that your Account has been accessed without your authorisation. Where we decide to close your Account we will provide you with notice of Account closure and where practicable, the reasons for closing your Account, together with the ability to withdraw any undisputed funds that we are holding." Paypal clearly identifies the effects of termination in section 7 of the ToS.

V. Section 4.1.5 – Variation of Contract Terms

	Variation of Contract Terms
500px	500px reserves the right, at its sole discretion, to modify or replace the terms at any time. If the alterations constitute a material change to the terms, 500px will notify you by posting an announcement on the site.
AWS	See section2 and 12 → AWS may modify agreement by posing a revised version on Site or by notifying Users. AWS will provide 90 days' advance notice in case of adverse changes to any SLA; in case of changes to/discontinuation of APIs, AWS will attempt to continue supporting the previous version of the API, except "if doing so (a) would pose a security or intellectual property issue, (b) is economically or technically burdensome, or (c) would cause us to violate the law or requests of governmental entities)."
ADRIVE	"ADrive may from time to time amend the terms and conditions of this Agreement. At the time of any such change, you will be notified of the modified terms and conditions."
Basecamp	"The Company reserves the right at any time and from time to time to modify or discontinue, temporarily or permanently, any part of the Service with or without notice. (…) The Company shall not be liable to you or to any third party for any modification, price change, suspension or discontinuance of the Service."
Datapipe	GoGrid may amend this Agreement, including any document incorporated by reference, from time to time by posting an amended version at its website and sending Customer written notice thereof, including without limitation notice by e-mail. Such amendment will be deemed accepted and become effective 30 days after such written notice unless Customer first gives GoGrid written notice that it objects to the amendment. In such case, this Agreement will continue under its original provisions until, and the amendment will become effective upon the first to occur of: (a) the start of the next Term beginning 45 or more days after written notice of the amendment (unless the Term does not renew pursuant to Section 7.1 above); or (b) the effective date of the next Order submitted by Customer after notice of the amendment and accepted by GoGrid. Customer's continued use of the Service following the effective date of an amendment will confirm Customer's consent thereto. This Agreement may not be amended in any other way except through a written agreement executed by each party. Notwithstanding the foregoing, a revision to the AUP, Privacy Policy, or SLA will be effective immediately, without right of rejection, if it does not materially reduce Customer's rights or increase its responsibilities. (Revision of uniform resource locators listed in this Agreement will not constitute an amendment.)
Dropbox	"If an update affects your use of the Services or your legal rights as a user of our Services, we'll notify you prior to the update's effective date by sending an email to the email address associated with your account or via an in-product notification. These updated Terms will be effective no less than 30 days from when we notify you. If you don't agree to the updates we make, please cancel your account before they become effective. Where applicable, we'll offer you a pro rata refund based on the amounts you have pre-paid for Services and your account cancellation date. By continuing to use or access the Services after the updates come into effect, you agree to be bound by the revised Terms."
Facebook	Facebook will notify users before making changes and allow users to review/comment on revised terms before. Changes to policies, guidelines or other terms referenced in the ToS may be provided on the Site Governance Page. Continued use of the Services, following notice of changes constitutes acceptance of amendments.

Google Drive	Changes on performance/security/functionalities/features, as follows: "We may make performance or security improvements, change functionalities or features, or make changes to comply with law or to prevent illegal activities on, or abuse of, our systems. You can subscribe to receive information about Google Drive here [https://drive.googleblog.com]. We will provide notice of material changes to Google Drive that we reasonably believe will adversely impact your use of Google Drive. However, there are times when we will need to make changes to Google Drive without giving notice. These will be limited to instances where we need to take action to ensure the security and operability of the service, prevent abuse or where we must act to meet legal requirements." Changes on plan/prices, as follows: "We may change the storage plan and price in effect but will give you prior notice of these changes. These changes will apply after your current service term expires, when the next payment is due from you after the notice. We will give you at least 30 days' prior notice of a price increase or storage plan decrease before you are charged. If you are given less than 30 days' prior notice, the change will not apply until the payment after the next payment is due. If you do not wish to continue with the updated storage plan or price, you may cancel or downgrade your Paid Storage Plan at any time from within your Google Drive storage settings. Your cancellation or downgrade will apply to the next billing period after the current service term; we will continue to make your files available to you or give you a chance to take your files out of Google Drive."
iCloud	"Apple reserves the right at any time to modify this Agreement and to impose new or additional terms or conditions on your use of the Service, provided that Apple will give you 30 days' advance notice of any material adverse change to the Service…" "With respect to paid cloud storage services, Apple will not make any material adverse change to the Service before the end of your current paid term (…) In the event that Apple does make material adverse changes to the Service or terms of use, you will have the right to terminate this Agreement and your account, in which case Apple will provide you with a pro rata refund of any pre-payment for your then-current paid term. Apple shall not be liable to you for any modifications to the Service or terms of service made in accordance with this Section IE
Instagram	"We reserve the right, in our sole discretion, to change these Terms of Use ("Updated Terms") from time to time. Unless we make a change for legal or administrative reasons, we will provide reasonable advance notice before the Updated Terms become effective. You agree that we may notify you of the Updated Terms by posting them on the Service, and that your use of the Service after the effective date of the Updated Terms (or engaging in such other conduct as we may reasonably specify) constitutes your agreement to the Updated Terms. Therefore, you should review these Terms of Use and any Updated Terms before using the Service. The Updated Terms will be effective as of the time of posting, or such later date as may be specified in the Updated Terms, and will apply to your use of the Service from that point forward. These Terms of Use will govern any disputes arising before the effective date of the Updated Terms."
Linode	Concerning the ToS, there are no provisions on the limits to changes, how they will occur or their consequences. References to changes/amendments are the ones below: "4.(…) Subscriber is aware that Linode.com may prospectively change the specified rates and charges from time to time. (…) 13. You agree that Linode.com may provide you with notices, including those regarding changes to the Terms of Service, by email, regular mail, or postings on Linode.com services. (…) 14. The Terms of Service (including any policies, guidelines or amendments that may be presented to you from time to time) constitute the entire agreement between you and Linode.com..:" On the PP: "Amendments to this privacy policy may be made at any time and you should check back frequently for any changes. Linode will never make changes to this policy that result in less protection of your personal information without sending notice. This policy was last updated on May 2nd, 2017." There is not a clear obligation to inform Users of changes.
MEGA	"3 We can change these terms at any time by providing you at least 30 days' prior notice of the change, whether via our website, via our mobile apps, by sending you an email or via any messaging service we provide. Your continued use after that notice means that you agree to the changed terms. If you have paid for a subscription that is due to expire after that 30 day notice period and you do not wish to continue to use our services under the new terms, you may terminate your subscription before the new terms come into force. We will then (but not otherwise) refund the unexpired portion of your subscription payment within 30 days and close your account." (…) "We can also change the fees for our services (other than those you have already contracted and paid for) at any time if we give you notice."
Microsoft OneDrive	"We'll inform you if we intend to change these Terms. We may change these Terms if it is necessary due to (i) applicable law, including, but not limited to, a change of such law; (ii) an advice and/or order based on applicable law; (iii) the evolution of the Services; (iv) technical reasons; (v) operational requirements or (vi) an advantageous change of terms for the user. We'll inform you of the intended change before it takes effect, either through the user interface, in an email message or through other reasonable means. We'll provide you the opportunity to cancel the Services at least 30 days before the change becomes effective. Using the Services after the changes become effective means you agree to the new terms. If you do not agree to the new terms, you must stop using the Services and close your Microsoft account and/or Skype account in accordance with section 4(a)(iv).

	We'll also expressly point to this fact when informing you about the intended change of these Terms. (…) We will notify you in advance if a change to the Services will cause you to lose access to Your Content. For paid Services, we'll also notify you in advance of other material changes to the Services. Except to the extent required by applicable law, we have no obligation to provide a re-download or replacement of any material, Digital Goods (defined in section 13(k)) or applications previously purchased. If we cancel a paid Service, we'll refund to you on a pro-rata basis the amount of payments that you've made corresponding to the portion of that Service remaining right before the cancellation." "Changes to OneDrive Service. We will notify you at least 30 days in advance if any change to free or paid OneDrive services will cause you to lose access to Your Content on OneDrive (…) If we reduce your OneDrive data storage limits or cancel the OneDrive service, you may cancel your paid subscription for OneDrive and we'll provide you with a pro-rated refund for such subscription. We will provide you at least 30-days' notice of any such change and you must cancel within the period set forth in the notice." Nonetheless, it is worth noting that Microsoft provides a change history for the Service Agreement and Privacy Statement.
Norton Online Backup	"You agree that Symantec may, in its sole discretion and from time to time, establish or amend general operating practices to maximize the operation and availability of the Service and to prevent abuses."(…) "No amendment to this Agreement will be binding unless evidenced by a writing signed by the party against whom it is sought to be enforced"
PayPal	"We may at any time amend, delete or add to this Agreement, including the Fees and other amounts which apply to your Account (as set out in Schedule 1) (a "Change") by giving notice of such Change by posting a revised version of this Agreement on the PayPal website(s). A Change will be made unilaterally by us and you will be deemed to have accepted the Change after you have received notice of it. We will give you 2 months' notice of any Change with the Change taking effect once the 2 month notice period has passed, except the 2 month notice period will not apply where a Change is required by the law or relates to the addition of a new service, extra functionality to the existing Service or any other change which neither reduces your rights nor increases your responsibilities. In such instances, the Change will be made without prior notice to you and shall be effective immediately. (…) If you do not accept any Change, you must close your Account following the account closure procedure set out in section 7 (Term and closing Your Account). If you do not object to a Change by closing your Account within the 2 month notice period, you will be deemed to have accepted it."

VI. Section 4.2.1 – Integrity and Data Preservation

	Integrity	**Data Preservation**
500px	"You use the Site and the Services at your own risk", and in the summary column it adds "always have a backup of your photos"	"Upon termination of your account 500px will automatically remove all Visual Content posted to your account."
AWS	"You are responsible for (…) taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content."	AWS does not guarantee the deletion of User's content, but allows Users to retrieve their data within 30 days after termination (refer to section on Retrieval).
ADRIVE	"ADrive shall have no responsibility for and does not guarantee the integrity, completeness or availability of ADrive Services or of Storage Data residing on ADrive's equipment. You are responsible for independent backup of Storage Data stored using the ADrive Services."; "Adrive recommends that any user of the Adrive services maintain an alternative storage medium to ensure that data is backed up to multiple locations."	"ADrive may, in its sole discretion, remove, reclassify, recategorize, or block Your access to all or any part of ADrive Services or to any particular Storage Data at any time for any reason, or for no reason at all."; "ADrive may, but shall not be required to, delete Your Storage Data after the termination of this Agreement."
Basecamp	"Your use of the Service is at your sole risk. The service is provided on an "as is" and "as available" basis." and "The Company does not warrant that (i) the service will meet your specific requirements, (ii) the service will be uninterrupted, timely, secure, or error-free (…) (v) any errors in the	"When you cancel your account, we'll ensure that nothing is stored on our servers past 30 days. Anything you delete on your account while it's active will also be purged within 30 days (up until then it's available in the trash can)."

	Service will be corrected."; however, Basecamp also states that: "Our servers — from power supplies to the internet connection to the air purifying systems — operate at full redundancy. Our systems are engineered to stay up even if multiple servers fail."[294]	
Datapipe	"In addition to any applicable SLA credits, GoGrid will make reasonable efforts to recover data lost as a result of hardware failures, upon Customer's request, but GoGrid does not guarantee data recovery."; ultimately, "Customer is responsible for maintaining the security of its data, even if GoGrid provides data security features of the Services." and (…) "responsible for maintaining security, including disaster recovery systems and backups. (Customer is advised to maintain its own backups outside of GoGrid's premises and systems, even if GoGrid provides backups, security, or other services related to data protection.)"	No specific commitment to delete data following termination
Dropbox	"The customer is responsible for (…) backing up any stored data on the services."	"If this Agreement is terminated: (b) Dropbox may, at the Customer's request, provide the Customer with access to its account at then-current fees so that the Customer may export its Customer Data; and (c) after a commercially reasonable period of time, Dropbox may delete any Customer Data relating to the Customer's account."
Facebook	No specific commitments on data integrity.	As per the ToS: "When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others)." As per the PP: "We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services." "You can delete your account any time. When you delete your account, we delete things you have posted, such as your photos and status updates"
Google Drive	"We don't make any commitments about the specific functionality available through Google Drive, its reliability, availability, or ability to meet your needs."	"We believe that you own your data and preserving your access to such data is important. If we discontinue a Service, where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service."; however, Google provides no specific commitment to delete data after termination of Services.[295]
iCloud	"You are responsible for backing up, to your own computer or other device, any important documents, images or other Content that you store or access via the Service. Apple shall use reasonable skill and due care in providing the Service, but Apple does not guarantee or warrant that any Content you may store or access through the Service will not be subject	"Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may pre-screen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable." Apple further adds that upon termination of account "…after a period of time, Apple will delete

[294] https://basecamp.com/about/policies/security

[295] Instead, Google indicates that it will give prior notice before discontinuation/ termination (with exceptions) for the user to retrieve his/her files, but is not clearly spelled out whether those are deleted after or not – this is relevant since the license provided to Google to use (and etc.) User's content continues unless a user delete his/her content, regardless of the use of the services.

	to inadvertent damage, corruption or loss." + "To the greatest extent permissible by applicable law, apple does not guarantee or warrant that any content you may store or access through the service will not be subject to inadvertent damage, corruption, loss, or removal in accordance with the terms of this agreement, and apple shall not be responsible should such damage, corruption, loss, or removal occur. it is your responsibility to maintain appropriate alternate backup of your information and data."	information and data stored in or as a part of your account(s)."
Instagram	No specific commitments on data integrity.	"Following termination or deactivation of your account, Instagram, its Affiliates, or its Service Providers may retain information (including your profile information) and User Content for a commercially reasonable time for backup, archival, and/or audit purposes"; nonetheless, Instagram indicates that "[w]hen you delete your account, your profile, photos, videos, comments, likes and followers will be permanently removed."[296]
Linode	Linode offers back-up services[297], but disclaims any warranties relating to it.	Commitment on deletion/preservation of data only pertains personal information, no specific commitments on User's content.
MEGA	"You must maintain copies of all data stored by you on our services. We do not make any guarantees that there will be no loss of data or the services will be bug free."	"If you choose to stop using our services, you need to make sure you download your data first because after that we may, if we wish, delete it. If we suspend our services to you because you have breached these terms, or someone you have given access to has breached these terms, during the term of that suspension, we may, if we wish, deny you access to your data but keep it for evidential purposes. If we terminate our services to you because you or someone you have given access to has breached these terms, we may, if we wish, delete your data immediately or keep it for evidential purposes. In circumstances where we cease providing our services for other reasons, we will, if reasonably practicable and we are not prevented by law or likely to incur any liability in doing so, give you 30 days' notice to retrieve your data."
Microsoft OneDrive	"To help protect your OneDrive files from hardware failure, we save multiple copies of each file on different drives and servers."[298]; nonetheless, Microsoft also highlights to Users that they "(…) should have a regular backup plan."	"If you violate any of the obligations listed in section 3(a(..) we may take action against you including (without limitation) (…)the right to remove or block Your Content from the Services at any time if it is brought to our attention that it may violate applicable law or these Terms."(…) "If you have more content stored in your OneDrive account than is provided to you under the terms of your free or paid subscription service for OneDrive and you do not respond to notice from Microsoft to fix your account by removing excess content or moving to a new subscription plan with more storage, we reserve the right to close your account and delete or disable access to Your Content on OneDrive." "Second, we'll delete Data or Your Content associated with your Microsoft account or Skype account or will otherwise disassociate it from you and your Microsoft account or Skype account (unless we are required by law to keep it). As a result you will no longer be able to access any of the Services (or

[296] https://help.instagram.com/139886812848894
[297] https://www.linode.com/backups
[298] https://support.office.com/en-us/article/OneDrive-file-security-23c6ea94-3608-48d7-8bf0-80e142edd1e1

		Your Content that you've stored on those Services) that require a Microsoft account.
Norton Online Backup	"Symantec assumes no responsibility for the deletion or failure to store Data. Symantec retains the right, at Symantec's sole discretion, to determine whether or not Your conduct is consistent with the terms of this Agreement and may terminate Your access to the Service if Your conduct is found to be in violation of the terms of this Agreement."	"Following the expiration or termination of the Service Period: - Data stored to the online backup space provided with Your Service will be at risk of being purged; - Symantec shall not be obligated to maintain such Data, forward such Data to You or a third party, or migrate such Data to another backup service or account; and"
PayPal	No specific commitments on data integrity.	"we may keep your Account information in our database for the purpose of fulfilling our legal obligations" (in UA, section 7); and "If you close your PayPal account, we will mark your account in our database as "Closed", but will keep your Account Information in our database. This is for instance necessary in order to deter fraud, by ensuring that persons who try to commit fraud will not be able to avoid detection simply by closing their account and opening a new account. However, if you close your account, your personally identifiable information will not be used by us for any further purposes, nor sold or shared with third parties, except as necessary to prevent fraud and assist law enforcement authorities, or as required by law."

VII. Section 4.2.2 – Disclosure/Confidentiality of Data

Disclosure/confidentiality of hosted data	
500px	On personal data: "We may release personal information when we believe in good faith that release is necessary to comply with a law; to enforce or apply our Terms of Use and other policies; or to protect the rights, property, or safety of 500px, our employees, our users, or others"; no details/commitments on disclosure limitations regarding other types of data.
AWS	"We do not disclose customer content unless we're required to do so to comply with the law or a valid and binding order of a governmental or regulatory body."[299] (…)Unless it would violate the law or a binding order of a governmental body, we will give you notice of any legal requirement or order referred to in this Section 3.2."
ADRIVE	"If ADrive believes, in its sole and absolute discretion, that You may be engaging in, or in any way connected with, any unlawful or improper activity, ADrive may disclose its Users' files and Storage Data to law enforcement or any other authority ADrive deems proper" (…)"ADrive does not guarantee the security of any information transmitted to or from ADrive."
Basecamp	"While we may be required to disclose your personal information (and data[300]) in response to a lawful request by public authorities, including to meet national security or law enforcement requirements, Basecamp won't otherwise hand your data over to law enforcement unless a court order says we have to. We flat-out reject such other requests from local and federal law enforcement when they seek data without a court order. And unless we're legally prevented from it, we'll always inform you when such requests are made."
Datapipe	"GoGrid is a passive recipient of Hosted Data: we take no active part in collecting it, and generally we do not access its content." (…) "GoGrid doesn't share personally identifiable information or Hosted Data under any circumstances, except (…) when requested by law enforcement agencies or required by law; to maintain security of network/services; to collect money owed to GoGrid; to identify, contact or take legal action against costumers/3rd parties for violation AUP/ breaking the law. (…) Also, independent contractors may have access to data, when assisting to run the Service."

[299] https://aws.amazon.com/compliance/eu-data-protection/ , What happens when AWS receives a legal request for customer content?
[300] https://basecamp.com/about/policies/privacy

Dropbox	"We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights. Stewardship of your data is critical to us and a responsibility that we embrace. We believe that our users' data should receive the same legal protection regardless of whether it's stored on our Services or on their home computer's hard drive. We'll abide by the following Government Request Principles when receiving, scrutinising and responding to government requests (including national security requests) for our users' data:"
Facebook	"We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; or to prevent death or imminent bodily harm."
Google Drive	Google may disclose data when it has " a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: (…) meet any applicable law, regulation, legal process or enforceable governmental request"; "enforce applicable Terms of Service, including investigation of potential violations"; "detect, prevent, or otherwise address fraud, security or technical issues"; protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law."
iCloud	"Apple reserves the right to take steps Apple believes are reasonably necessary or appropriate to enforce and/or verify compliance with any part of this Agreement. You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate, if legally required to do so or if Apple has a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b) enforce this Agreement, including investigation of any potential violation thereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law."
Instagram	"Except as otherwise described in the Service's Privacy Policy(…) any Content will be non-confidential and non-proprietary and we will not be liable for any use or disclosure of Content. You acknowledge and agree that your relationship with Instagram is not a confidential, fiduciary, or other type of special relationship, and that your decision to submit any Content does not place Instagram in a position that is any different from the position held by members of the general public, including with regard to your Content. None of your Content will be subject to any obligation of confidence on the part of Instagram, and Instagram will not be liable for any use or disclosure of any Content you provide." "We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm."
Linode	"The Terms of Service specifically prohibits the use of our service for illegal activities. Therefore, Subscriber agrees that Linode.com may disclose any and all subscriber information including assigned IP numbers, account history, account use, etc. to any court who sends us a valid Court Order, without further consent or notification to the Subscriber."
MEGA	"We reserve the right to disclose data and other information as required by law or any competent authority. Our approach is referenced in our Privacy Policy and Takedown Guidance Policy both of which are subject to these terms."; as per PP: "10 A user's data is encrypted by the user before upload to our system and therefore we do not and cannot access that content unless we are provided with the decryption key. A user may give access to others by providing them with a link and decryption key and shall be responsible for their compliance with this Policy. 11 If we think it is necessary or we have to by law in any jurisdiction then we are entitled to give a user's information to competent authorities. We reserve the right to assist any law enforcement agency with investigations, including disclosure of information to them or their agents. We also reserve the right to comply with any legal processes, including but not limited to subpoenas, search warrants and court orders initiated by enforcement authorities or other third parties. We may disclose a user's information to enforce or apply our Terms or any other agreement we have with that user; or to protect the rights, property, or safety of us or our other users, third parties

	or the operation of our services and the website. For more detail on disclosure to competent enforcement authorities and other third parties, see our Takedown Guidance Policy. (…) 13 Other than as set out above, we will not sell or otherwise provide users' personal information to a third party, or make any other use of personal information for any purpose which is not specifically allowed under this Policy or our Terms or is not incidental to the normal use of our services."
Microsoft OneDrive	"Finally, we will (…) disclose, and preserve personal data, including your content (…), when we have a good faith belief that doing so is necessary to: (i) comply with applicable law or respond to valid legal process (…) ;(ii) protect our customers, for example to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone; (iii) operate and maintain the security of our products, (…); or protect the rights or property of Microsoft (…) however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement."
Norton Online Backup	"Symantec reserves the right to cooperate with any legal process and any law enforcement or other government inquiry related to your use of this Software. This means that Symantec may provide documents and information relevant to a court subpoena or to a law enforcement or other government investigation (…) Symantec reserves the right at all times to monitor, review, retain and/or disclose any Data or other information as necessary to satisfy any applicable law, regulation, legal process or governmental request, or to investigate any suspected breach of these Terms and Conditions."
PayPal	Paypal discloses data to financial/payment service (listed quarterly in its website) providers from time to time so that services can be performed; additionallly, Paypal may disclose information to "police and other law enforcement agencies and other third parties (…) that (i) we are legally compelled and permitted to comply with (…)"; (ii) we have reason to believe it is appropriate for us to cooperate with in investigations of fraud or other illegal activity or potential illegal activity, or (iii) to conduct investigations of violations of our User Agreement (including without limitation, your funding source or credit or debit card provider)", as well as to IPR owners, if they state to have a claim against Paypal due to infringement of their IPRs carried out through the use of Paypal Services.

VIII. Section 4.2.3 – Transfer and Location of Data

	Transfer and Location of Data
500px	No information provided on transfer or location of data.
AWS	AWS allows users to select the regions in which their Content is stored and that it will not move it, unless if necessary to comply with the law or a binding order of a governmental body. Users "consent to the storage of Your Content in, and transfer of Your Content into the AWS regions you select (…)" and AWS "will not (b) subject to Section 3.3, move Your Content from the AWS regions selected by you; except in each case as necessary to comply with the law or a binding order of a governmental body."
ADRIVE	No information provided on transfer or location of data.
Basecamp	No information provided on transfer or location of data.
Datapipe	Data centres are located in in Europe; no specific provisions on transfers of data.
Dropbox	No specific information on where data is located; in addition,, "The Customer agrees that Dropbox and its Sub-processors may transfer, store and process Customer Data in locations other than the Customer's country."
Facebook	The ToS (sect. 16.1) indicates that that personal data is transferred to and processed in the United States; on transfer the PP states that "Facebook may share information internally within our family of companies or with third parties for purposes described in this policy. Information collected within the European Economic Area ("EEA") may, for example, be transferred to countries outside of the EEA for the purposes as described in this policy."
Google Drive	No information provided on transfer or location of data.
iCloud	No information on location of data; on transfer, PP states: "All the information you provide may be transferred or accessed by entities around the world as described in this Privacy Policy. Apple uses approved Model Contractual Clauses for the international transfer of personal information collected in the European Economic Area and Switzerland."
Instagram	"Your information collected through the Service may be stored and processed in the United States or any other country in which Instagram, its Affiliates or Service Providers

	maintain facilities." "Instagram, its Affiliates, or Service Providers may transfer information that we collect about you, including personal information across borders and from your country or jurisdiction to other countries or jurisdictions around the world."
Linode	Linode allows users the possibility to use a location of their choosing (e.g. EU location); however, it is not clear whether if such data will be transferred to other locations (e.g. for back-up or better performance purposes).
MEGA	No information provided on transfer or location of data.
Microsoft OneDrive	"Personal data collected by Microsoft may be stored and processed in your region, in the United States or in any other country where Microsoft or its affiliates, subsidiaries or service providers maintain facilities. Microsoft maintains major data centers in the United States, Canada, Brazil, Ireland, the Netherlands, Austria, Finland, India, Singapore, Malaysia, Hong Kong, Japan, and Australia. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located."; "When we transfer personal data from the European Economic Area and Switzerland to other countries, some of which have not been determined by the European Commission to have an adequate level of data protection. When we do, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data."
Norton Online Backup	"By using the Service, You acknowledge and agree that Symantec may collect, transmit, store, disclose and analyze such information for these purposes. In addition, any Data that You transmit or store through the Service may be transferred to the Symantec group in the United States or other countries that have less protective data protection laws than the region in which You are situated (including outside the European Economic Area), but Symantec has taken steps so that the Data, if transferred, receives an adequate level of protection, including by using data transfer agreements where required."
PayPal	No information on location of data; however, data may be transferred to "non-EEA member states", if required by law, or to 3rd parties providing services/PayPal group entities.

IX. Section 4.2.4 – Retrieval on Termination

	Retrieval on Termination
500px	"It is your responsibility to remove all Visual Content from your account prior to termination. Upon termination of your account 500px will automatically remove all Visual Content posted to your account." However, since an account may be terminated "immediately, without prior notice or liability, for any reason whatsoever" and that "[u]pon termination of your account, your right to use the Services will immediately cease", Users might be unable to retrieve their data.
AWS	Users have 30 days after termination date, if User has paid amounts due under the Agreement.
ADRIVE	ADrive does not ensure the possibility to retrieve user's content after termination for convenience or for cause.
Basecamp	"All of your content will be inaccessible from the Service immediately upon cancellation. Within 30 days, all Basecamp 3 content will be permanently deleted from all backups and logs."
Datapipe	"GoGrid is not responsible for providing physical access to or copies of software, data, or content stored on GoGrid's equipment under any circumstances and is not required to provide network access (a) after any termination or suspension of Services…"; however, if using the ColoServer, "Customer will remove any and all equipment Customer has placed in the Space or elsewhere in the Facility, promptly after GoGrid so directs, and in any case within 3 business days of termination."
Dropbox	"We'll provide you with reasonable advance notice via the email address associated with your account to remedy the activity that prompted us to contact you and give you the opportunity to export Your Stuff from our Services."
Facebook	Once accounts are terminated their data is no longer accessible; nonetheless, users are recalled of the possibility to download a copy of their data prior to terminating the account, unless Facebook terminates their account for cause.

Google Drive	In case of termination by Google, it will provide prior notice of suspending/disabling access to the account, during which period the User should retrieve the files; in case of discontinuation of services, a 60-days' prior notice days will be given for the user to retrieve files. In case of cancellation/downgrade following plan/price change, Google "will continue to make your files available to you or give you a chance to take your files out of Google Drive."
iCloud	Apple is allowed to terminate/suspend an account immediately. In limited cases, will it provide a 30 days' notice, thereby allowing Users to retrieve their content; however, retrieval of data upon termination is not guaranteed.
Instagram	User's content will become inaccessible after termination of the services.
Linode	Linode does not grant users the possibility to retrieve their content upon termination, but it states that it will use "reasonable care in notifying the Customer" and that "[i]f at any time it becomes necessary for Linode.com to cancel a customer's service without cause, Linode.com will provide 30 days advance notice".
MEGA	"In circumstances where we cease providing our services for other reasons [i.e. those not relating to User's own account cancellation or breach of terms] we will, if reasonably practicable and we are not prevented by law or likely to incur any liability in doing so, give you 30 days' notice to retrieve your data."
Microsoft OneDrive	Microsoft does not ensure retrieval upon termination, stating that users "may lose access to and use of your account when you cancel the Services" or that Microsoft "reserve the right to close your account and delete or disable access to Your Content on OneDrive."; however, it also states that, following a user's request for termination, the account will remain "in a suspended state for 60 days just in case you change your mind.", which indicates that the data is kept for at least this period, even though it is not clear whether users are allowed to retrieve it, without re-activation of the services.
Norton Online Backup	"Following the expiration or termination of the Service Period: Data stored to the online backup space provided with Your Service will be at risk of being purged; Symantec shall not be obligated to maintain such Data, forward such Data to You or a third party, or migrate such Data to another backup service or account"
PayPal	Paypal does not ensure the possibility to retrieve user's content after termination.

X. Section 4.2.5 –Data Protection

	Data Protection
500px	500px indicates that it will neither rent nor sell User personal information, however, this provides numerous exclusions, namely that " 500px may choose to buy or sell assets and that user information is one of those assets that is transferred, may share user info with 3rd parties (that help to provide services), and that 500px will contact users when personal information is shared with 3rd parties or used for a purpose incompatible with the original one, allowing users to opt out.
AWS	AWS shares "customer information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice." It may also share such information with 3rd party service provides (that it employs to perform services on its behalf); in view of a business transfer and in order to comply with law/enforce conditions or protect rights/property/safety of Amazon, their users or other. AWS indicates that it complies with the EU Data Protection rules, namely by providing encryption possibilities and the possibility to manage their own encryption keys. [301] AWS adds it does not "access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users. We never use customer content or derive information from it for marketing or advertising." AWS was a participant to the EU-US Privacy Shield framework.
ADRIVE	"ADrive will not give, sell, rent, share, or trade any personal information about You to third parties or provide Your personal information, including your name or electronic mail address, to third parties except as required by law, subpoena or court order, and/or as ADrive believes necessary or appropriate in connection with an investigation for fraud…"; h**owever**, "ADrive may share aggregated demographic information with its partners and advertisers." and ADrive may rent, sell or otherwise share metadata provided in connec-

[301] https://aws.amazon.com/compliance/eu-data-protection/

	tion with the User's Storage Data with other entities at its discretion".
Basecamp	"We'll never sell your personal info to third parties, and we won't use your name or company in marketing statements without your permission, either. (…) You always have the right to access the personal information we store about you. (…) Basecamp does not share individual's personal data with non-agent third parties. If this policy changes in the future, we will notify individuals and provide them with an opportunity to opt-out of having their data shared. (…) Basecamp complies with the EU-US Privacy Shield Framework (…) regarding the collection, use, and retention of personal information from European Union member countries (…) "In cases of onward transfer to these third parties for data of EU individuals received pursuant to the EU-US Privacy Shield, Basecamp is potentially liable should any issues or concerns arise."
Datapipe	"GoGrid does not sell or rent personally identifiable information." (...) GoGrid doesn't share personally identifiable information or Hosted Data under any circumstances, except" when: (i) log replies or contest sign-ups include personally identifiable information, (ii) requested by law enforcement agencies or required by law; (iii) to maintain security of network/services; (iv) to collect money owed to GoGrid; (v) to identify, contact or take legal action against costumers/3rd parties for violation AUP/ breaking the law. Also, independent contractors may have access to data, when assisting to run the Service." GoGrid was a participant to the EU-US Privacy Shield.
Dropbox	"To the extent that Dropbox, Inc. is, on behalf of the Customer, processing Customer Data that is subject to EU Data Protection Laws, by clicking "I agree", you are also agreeing to the EU Standard Contractual Clauses, defined below, with Dropbox, Inc. for the transfer of personal data to processors. (…) Dropbox and its Sub-processors will only process Customer Data to provide the Services and to fulfil Dropbox's obligations under the Agreement. Sub-processors' processing activities will be restricted to processing on Dropbox's behalf and in accordance with Dropbox's instructions. The Customer agrees that Dropbox and its Sub-processors may transfer, store and process Customer Data in locations other than the Customer's country". Dropbox was a participant to the EU-US Privacy Shield.
Facebook	Facebook processes the following data: "Things you do and information you provide. Things others do and information they provide. Your networks and connections. Information about payments. Device information. Information from websites and apps that use our Services. Information from third-party partners"; such data can be shared with "People you share and communicate with. People that see content others share about you. Apps, websites and third-party integrations on or using our Services" (…) When sharing data with 3rd party companies for Advertising, Measurement and Analytics Services, Facebook does not provide Personally Identifiable Info. Vendors, service providers or other partners, supporting Facebook's business, also receive information, but must adhere to strict confidentiality obligations". Facebook is certified by TRUSTe and was a participant to the EU-U.S. Privacy Shield.
Google Drive	Google does not share personal information with companies, organizations and individuals outside of Google, except in the certain cases (e.g. user consent, for external processing, as a result of a legally enforceable request); in any case, Google "may share non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites." Google has also adhered to several self-regulatory frameworks (https://www.google.com/policies/privacy/frameworks/), including the EU-US and Swiss-US Privacy Shield.
iCloud	"We collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose (…) We treat information collected by cookies and other technologies as non-personal information. However, to the extent that Internet Protocol (IP) addresses or similar identifiers are considered personal information by local law, we also treat these identifiers as personal information. Similarly, to the extent that non-personal information is combined with personal information, we treat the combined information as personal information for the purposes of this Privacy Policy." Regarding disclosure to other parties, Apple indicates that "Personal information will only be shared by Apple to provide or improve our products, services and advertising; it will not be shared with third parties for their marketing purposes."; when Apple shares personal information with companies who provide services to it such entities are also obliged "to protect your information and may be located wherever Apple operates". Concerning **transfer of personal data, it :** "All the information you provide may be transferred or accessed by entities around the world as described in this Privacy Policy. Apple uses approved Model Contractual Clauses for the international transfer of personal information collected in the European Economic Area and Switzerland. Apple, as a global company, has a number of legal entities in different jurisdictions which are responsible for the personal information which they collect and which is processed on their behalf by Apple Inc.".

Instagram	"Instagram, its Affiliates, or Service Providers may transfer information that we collect about you, including personal information across borders and from your country or jurisdiction to other countries or jurisdictions around the world. If you are located in the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that we may transfer information, including personal information, to a country and jurisdiction that does not have the same data protection laws as your jurisdiction."
Linode	"Linode (…) collects and stores personal information, including the full name, company name (if applicable), billing address, credit card number and expiration date, email address, and source IP address for all customers.", as well as cookies through the use of Google Analytics; in relation to transfer of personal information to 3rd parties, "Linode discloses the full name, billing address, and credit card account information of its customers to a third-party merchant processing provider for billing purposes. Linode does not disclose customer information to other third parties (…) Linode discloses the billing address, network IP address, and a partial credit card number (for issuing bank identification purposes) of customers to a third party as part of the sign-up process for fraud detection purposes" In addition, Linoe states that "Customers shall have the right to opt out of any use of their personal information which is inconsistent with or beyond the scope of the purposes for which it was initially collected. In the event that, at Linode's discretion, service cannot be continued without customer acceptance of such modifications to the ways in which personal information is collected and/or used, customers who wish to opt out of such collection or use of their personal information will be notified and offered a pro-rated refund of any positive balance on their account with Linode". Lastly, Linode indicates that "Customers are solely responsible for ensuring compliance with any and all applicable privacy guidelines and regulations for all jurisdictions in which they may operate with respect to appropriate practices for the collection, storage, and dissemination of personal information using their Linode VPS. In no event shall Linode be held liable for a customer's failure to adopt and/or practice appropriate measures for safeguarding personal information stored within or transmitted through their Linode VPS."
MEGA	MEGA collects data given on registration (name, surname, email), IP address, data generated when using the services, namely: activity log, files uploaded, metadata about files, email address of persons with who file is shared, IP address from which the file was uploaded, account and payment info and direct comms between user and MEGA. Info is also collected by Cookies, which MEGA may: (i) join with users' info to provide to advertisers, without personally identifying any user; (ii) analyse and use for marketing or statistical purposes or to improve business; (iii) to serve advertisements/use 3rd party advertisers to serve ads on the Site. Additionally, MEGA commits to "keep a user's data and personal information while they are subscribed to our services (…)" and it "may, but shall not be obliged to, keep data and information after a user's account has been suspended or terminated (…) where we consider it necessary for evidential purposes relating to a breach of our Terms or with respect to current or anticipated action by any competent enforcement authority or other third party."
Microsoft OneDrive	"We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. (…) In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. (…) Finally, we will access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary" (see section on Disclosure above). In addition for its European users, "Microsoft adheres to applicable data protection laws in the European Economic Area, which if applicable includes the following rights: (i) If the processing of personal data is based on your consent, you have a right to withdraw consent at any time for future processing; (ii) You have a right to request from us, a "data controller" as defined in the law, access to and rectification of your personal data; (iii) You have a right to object to the processing of your personal data; and; (iv)You have a right to lodge a complaint with a data protection authority. (…) When we process personal data about you, we do so with your consent and/or as necessary to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfil other legitimate interests of Microsoft (…) When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms (…)."
Norton Online Backup	"Any Data that You transmit or store through the Service may be transferred to the Symantec group in the United States or other countries that have less protective data protection laws than the region in which You are situated (including outside the European Economic Area), but Symantec has taken steps so that the Data, if transferred, receives an adequate level of protection, including by using data transfer agreements where required"; "We do not sell, lease, rent or give away Your Information. We only disclose Your Information as described below, within our group of companies, with our partners, with service providers that process information on our behalf and with law enforcement. Processing is only undertaken for the purposes described in this Statement. If we disclose Your Information, we require those we disclose it with to comply with adequate privacy

	and confidentiality requirements and security standards.”**;** “We retain Your Information for as long as your account is active or as needed to provide you services. We also retain and use Your Information as necessary to comply with our legal obligations, resolve disputes and enforce our agreements. We store Your Information for as long as is necessary for the purpose for which we collect it.”; Users may view/update/correct information and may request the removal of inaccurate or incorrect info Symantec has on them..
PayPal	Paypal discloses data to financial/payment service providers to ensure performance of services; Paypal also lists 3rd party providers to whom they may disclose data and users expressly consent to transfer their data to those 3rd parties for the purposes listed therein. Nonetheless, “PayPal will not sell or rent any of your personal information to third parties for their marketing purposes without your explicit consent, and will only disclose this information in the limited circumstances and for the purposes described in this Privacy Policy. This includes transfers of data to non-EEA member states. Paypal may also transfer certain information to other PayPal group entities”. Moreover, Paypal may disclose information to “police and other law enforcement agencies and other third parties, including PayPal Group companies, that (i) we are legally compelled and permitted to comply with (…) (ii) we have reason to believe it is appropriate for us to cooperate with in investigations of fraud or other illegal activity or potential illegal activity, or (iii) to conduct investigations of violations of our User Agreement…”. Users may review the personal data that PayPal has on them and make changes to it.

XI. Section 4.2.6 and 4.2.7 – Security Requirements and Audit Rights

	Security Requirements	**Audit Rights**
500px	“Photos will be stored safely with enterprise-level security.”[302]	No specific commitments on possibility to conduct audits.
AWS	Amazon indicates that it has implemented “reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.”; in this sense, we highlight that AWS has the following certifications : ISO 9001, 27001, 27017, 27018, as well as BSI’s C5 (Germany)[303] and Cyber Essential Plus (UK)[304].	Users are not allowed to conduct audits, but may conducting penetration tests.[305]
ADRIVE	“ADrive uses available best practices to protect our Users' information. When ADrive asks Users to enter sensitive information (such as credit card number), that information is protected with SSL encryption software for transmission to ADrive. All of our Users' information is restricted in our offices. Only employees or contractors who need the information to perform a specific job are granted access to personally identifiable information.”; nonetheless, “ADrive does not guarantee the security of any information transmitted to or from ADrive.”	No specific commitments on possibility to conduct audits.
Basecamp	When announcing its services, Basecamp indicates that all data is encrypted via SSL/TLS when transmitted to their servers to a user’s browser and further indicates it ensures full redundancy for all major systems, sophisticated physical security, regular updates to its infrastructure and it states that its services are PCI-compliant.[306]	No specific commitments on possibility to conduct audits.
Datapipe	Datapipe indicates that most of its data centres are ISO 27001 certified and 24/7 physical onsite security.	No specific commitments on possibility to conduct audits.
Dropbox	Dropbox will use, as a minimum, industry standard technical and organisational security measures to transfer, store and process Customer Data. These measures are designed to protect the integrity of Customer Data and guard against the unauthorised or unlawful access to, use of	No specific commitments on possibility to conduct audits.

[302] See https://support.500px.com/hc/en-us/articles/221168807-500px-me-Frequently-Asked-Questions.
[303] See https://aws.amazon.com/compliance/bsi-c5/
[304] See https://aws.amazon.com/compliance/cyber-essentials-plus/
[305] See https://aws.amazon.com/security/penetration-testing/ .
[306] PCI (Payment Card Industry)-Compliance refers to the Data Security Standard (DSS) that applies to organizations that process, store, or transmit credit card information.

	and processing of Customer Data.	
Facebook	Facebook provides tips for Users to keep their accounts safe, however, no information was available concerning the type of measures implemented to ensure security of their overall system.	No specific commitments on possibility to conduct audits.
Google Drive	"We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular: We encrypt many of our services using SSL. We offer you two-step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome. We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems. We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.	No specific commitments on possibility to conduct audits.
iCloud	"Apple takes the security of your personal information very seriously. Apple online services such as the Apple Online Store and iTunes Store protect your personal information during transit using encryption such as Transport Layer Security (TLS). When your personal data is stored by Apple, we use computer systems with limited access housed in facilities using physical security measures. iCloud data is stored in encrypted form including when we utilize third-party storage."	No specific commitments on possibility to conduct audits.
Instagram	"We use commercially reasonable safeguards to help keep the information collected through the Service secure and take reasonable steps (such as requesting a unique password) to verify your identity before granting you access to your account. However, Instagram cannot ensure the security of any information you transmit to Instagram or guarantee that information on the Service may not be accessed, disclosed, altered, or destroyed."	No specific commitments on possibility to conduct audits.
Linode	"2. Linode employs industry-standard technical safeguards, including but not necessarily limited to encryption of credit card information, password and/or cryptographic key-based authentication controls on servers which house personal information, browser-based SSL encryption, and other storage system access control mechanisms to protect the integrity of internal databases and prevent unauthorized access." (…) "Linode as a company is PCI Data Security Standard (PCI DSS) compliant, which has been validated by an authorized independent Qualified Security Assessor."	No specific commitments on possibility to conduct audits.
MEGA	MEGA is known for its end-to-end encryption and for not having access to user's data. According to its general information "MEGA provides robust cloud storage with convenient and powerful always-on privacy. MEGA believes in your right to privacy and provides you with the technology tools to protect it. We call it User Controlled Encryption, or UCE, and it happens automatically." (…) "All files stored on MEGA are encrypted. All data transfers from and to MEGA are encrypted. And while most cloud storage providers can and do claim the same, MEGA is different – unlike the industry norm where the cloud storage provider holds the decryption key, with MEGA, you control the encryption, you hold the keys, and you decide who you grant or deny access to your files, without requiring any risky software installs"	No specific commitments on possibility to conduct audits.
Microsoft OneDrive	"Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption." Users may further enable two-step verification mechanisms.[307]	No specific commitments on possibility to conduct audits.
Norton Online Backup	Symantec includes indicates it has implemented physical safeguards (e.g. "controlled access to our facilities and secure destruction of media containing your information"), technology safeguards (e.g. use of Symantec anti-virus and endpoint protection software, encryption, and monitoring of our systems and data centers to and transmission of data using TLS encryption) and organizational safeguards (e.g. training and awareness programs on security and privacy, to make sure employees understand the importance and means by which they must protect users'	No specific commitments on possibility to conduct audits.

[307] https://support.microsoft.com/en-us/help/12408/microsoft-account-about-two-step-verification

	data).	
PayPal	"PayPal is committed to handling your customer information with high standards of information security. We use computer safeguards such as firewalls and data encryption, we enforce physical access controls to our buildings and files, and we authorise access to personal information only for those employees who require it to fulfil their job responsibilities."; additionally, in its Safety Advice page, Paypal indicates that it provides personal data privacy, 24/7 monitoring of its infrastructure, and secure technology (encrypting online transactions heavily from start to finish). In addition, Paypal runs a bug bounty program to assist it with maintaining the service and its costumers secure.[308]	No specific commitments on possibility to conduct audits.

XII. Section 4.3.1 – Warranties

	Warranties
500px	500px disclaims all responsibility and liability for any damage resulting from the use of the service; the use of site and its services are provided on an "as is, as available" basis.
AWS	AWS indicates that services offerings are provided "as is" and makes no representations or warranties of any kind, disclaiming all warranties, implied or express.
ADRIVE	Adrive services are "provided "as is" and "as available", and Adrive further disclaims all such warranties, express or implied, to the fullest extent permissible by applicable law.
Basecamp	"The Company does not warrant that (i) the service will meet your specific requirements, (ii) the service will be uninterrupted, timely, secure, or error-free, (iii) the results that may be obtained from the use of the service will be accurate or reliable, (iv) the quality of any products, services, information, or other material purchased or obtained by you through the service will meet your expectations, and (v) any errors in the Service will be corrected".
Datapipe	"Gogrid makes no warranties, either express or implied, including without limitation any implied warranties of merchantability, fitness for a particular purpose…"
Dropbox	"To the fullest extent permitted by law, Dropbox and its affiliates (…) make no warranties, either express or implied, about the services. the services are provided "as is". We also disclaim any warranties of merchantability, fitness for a particular purpose and non-infringement".
Facebook	"We are providing Facebook AS IS without any express or implied warranties (…) We do not guarantee that Facebook will always be safe, secure or error-free or that Facebook will always function without disruptions, delays or imperfections".
Google Drive	"Other than as expressly stated, we don't make any commitments about the specific functionality available through Google Drive, its reliability, availability, or ability to meet your needs".
iCloud	"Some jurisdictions do not allow the exclusion of certain warranties, as such, to the extent such exclusions are specifically prohibited by applicable law, some of the exclusions set forth below may not apply to you. (…) Apple shall use reasonable skill and due care in providing the service. The following disclaimers are subject to this express warranty. Apple does not guarantee, represent, or warrant that your use of the service will be uninterrupted or error-free, and you agree that from time to time Apple may remove the service for indefinite periods of time, or cancel the service in accordance with the terms of this agreement. You expressly understand and agree that the service is provided on an "as is" and "as available" basis. Apple (…) expressly disclaim all warranties of any kind, whether express or implied".
Instagram	"The service, including, without limitation, Instagram content, is provided on an "as is", "as available" and "with all faults" basis. To the fullest extent permissible by law, neither Instagram nor its parent company nor any of their employees, managers, officers or agents (collectively, the "Instagram parties") make any representations or warranties or endorsements of any kind whatsoever, express or implied (…) The Instagram Parties hereby disclaim all warranties, express or implied, including, but not limited to, the warranties of merchantability, fitness for a particular purpose, non-infringement, title, custom, trade, quiet enjoyment, system integration and freedom from computer virus. (…) The Instagram parties do not represent or warrant that the service will be error-free or uninterrupted; that defects will be corrected; or that the service or the server that makes the service available is free from any harmful components, including, without limitation, viruses.(…) You acknowledge that your use of the service is at your sole risk."

[308] https://www.paypal.com/us/webapps/mpp/security-tools/reporting-security-issues#bounty-payments

Linode	"9. (…) Linode.com does not make implied or written warranties for any of our services. Linode.com denies any warranty or merchantability for a specific purpose. This includes loss of data resulting from delays, non-deliveries, wrong delivery, and any and all service interruptions caused by Linode.com. (…) 11. You agree that your use of Linode.com shall be at your sole risk. All services provided by Linode.com are available as is, without warranty."
MEGA	"We don't give you any warranty or undertaking about the services or the website which are provided "AS IS". To avoid doubt, all implied conditions or warranties are excluded as much as is permitted by law, including (without limitation) warranties of merchantability, fitness for purpose, safety, reliability, durability, title and non-infringement."
Microsoft OneDrive	"If you are a consumer, you have certain rights under the law. These rights include an obligation on Microsoft to provide the Services using reasonable care and skill. Nothing in these terms is intended to limit or exclude our liability for any breach by Microsoft of this. Except in cases in which we have hidden defects in bad faith or defects have rendered use of the services impossible and except for skype paid products, we provide the services "as is," "with all faults" and "as available." (…) We and our affiliates, resellers, distributors and vendors give no contractual guarantees or conditions. You have all mandatory warranties foreseen by law, but we grant no other warranties. We exclude any implied mandatory warranties, including those of merchantability, fitness for a particular purpose, (…) to the maximum extent permitted by applicable law.
Norton Online Backup	"To the maximum extent permissible under applicable law, the software and service and any third party software or service are provided on an "AS IS" and "AS AVAILABLE" basis, with all faults. Symantec and its licensors provide the service without warranties of any kind, written or oral, statutory, either express or implied. (…) Symantec and its licensors do not warrant that the service or software will be uninterrupted, error-free, or secure."
PayPal	"We provide to you the Services, our infrastructure, our websites, our software, and systems (…) whether operated by us or on our behalf subject to your statutory rights but otherwise without any warranty or condition, express or implied"

XIII. Section 4.3.2 – Exclusions

	Exclusion
500px	Except were provided by law 500px shall not be liable for any direct, indirect, incidental , punitive, consequential damages from the use or inability to use the site or services. Furthermore, the ToS limits users' possibility to pursue a class action or similar.
AWS	AWS shall not be liable for any direct, indirect, incidental, punitive, consequential or exemplary damages, even if a party has been advised of the possibility of such damages.
ADRIVE	**"**You agree that, except as otherwise expressly provided in this agreement, under no circumstances, including (but not limited to) negligence, shall ADrive be liable for any damages (including, but not limited to, direct, actual, incidental, indirect, special, punitive, or consequential damages) that relate to or result from the use of, the inability to use, or the corruption of storage data, or other data stored on, stored in, retrieved from, acquired, transmitted or transferred through ADrive services…"
Basecamp	"the Company shall not be liable for any direct, indirect, incidental, special, consequential or exemplary damages."
Datapipe	"Gogrid will have no liability to customer for any consequential, indirect, special, incidental, or punitive damages."
Dropbox	"We don't exclude or limit our liability to you where it would be illegal to do so – this includes any liability for Dropbox's or its affiliates' fraud or fraudulent misrepresentation in providing the services. In countries where the following types of exclusions aren't allowed, we're responsible to you only for losses and damages that are a reasonably foreseeable result of our failure to use reasonable care and skill, or our breach of our contract with you. This paragraph doesn't affect consumer rights that can't be waived or limited by any contract or agreement. (…) In countries where exclusions or limitations of liability are allowed, Dropbox, its affiliates, suppliers or distributors won't be liable for: (i) any indirect, special, incidental, punitive, exemplary or consequential damages, or (ii) any loss of use, data, business or profits, regardless of legal theory. These exclusions or limitations will apply regardless of whether or not Dropbox or any of its affiliates have been warned of the possibility of such damages. If you use the services for any commercial, business or resale purposes, Dropbox and its affiliates, suppliers or distributors will have no liability to you for any loss of profit, loss of business, business interruption or loss of business opportunity. Dropbox and its affiliates are not responsible for the conduct, whether online or offline, of any users of the services."
Facebook	"We will not be liable to you for any lost profits or other consequential, special, indirect, or incidental damages arising out of or in connection with this statement [i.e. 3rd party actions] or Facebook, even if we have been advised of the possibility of such damages. (…) "Applicable law may not allow the limitation or exclusion of liability or incidental or

	consequential damages, so the above limitation or exclusion may not apply to you. in such cases, Facebook's liability will be limited to the fullest extent permitted by applicable law."
Google Drive	"Google and its suppliers and distributors are not responsible or liable for: (a) losses that were not caused by our breach of these Terms; (b) any loss or damage that was not, at the time the relevant contract with you was formed, a reasonably foreseeable consequence of Google breaching the Terms; or (c) losses relating to any business of yours including lost profits, revenues, opportunity or data."
iCloud	"Some jurisdictions do not allow the exclusion or limitation of liability by service providers. To the extent such exclusions or limitations are specifically prohibited by applicable law, some of the exclusions or limitations set forth below may not apply to you. (…) You expressly understand and agree that Apple and its affiliates (…) shall not be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages (…) Apple shall use reasonable skill and due care in providing the service. The following limitations do not apply in respect of loss resulting from (a) Apple's failure to use reasonable skill and due care; (b) Apple's gross negligence, wilful misconduct or fraud; or (c) death or personal injury.
Instagram	"Under no circumstances will the Instagram parties be liable to you for any loss or damages of any kind (including, without limitation, for any direct, indirect, economic, exemplary, special, punitive, incidental or consequential losses or damages) that are directly or indirectly related to: (a) the service; (b) the Instagram content; (c) user content; (d) your use of, inability to use, or the performance of the service…"
Linode	"Linode.com shall not be liable for any damages arising from such causes beyond the direct and exclusive control of Linode.com. (…) In no event shall Linode.com be liable for any special or consequential damages, loss or injury. Linode.com is not responsible for any damages your business may suffer."
MEGA	"To the maximum extent permitted by law, we (…) are not liable whether in contract, tort (including negligence), equity or on any other grounds to you or anyone else for any direct, indirect or consequential damage, (…) occurring directly or indirectly from the use or ability or inability to use, or reliance on, our website, or the service and based on any type of liability including breach of contract, breach of warranty, tort (including negligence), product liability or otherwise."
Microsoft OneDrive	"**a.** Microsoft shall not be liable for Your Content, material or other third party material, including links to third-party websites and activities provided by users. Such content and activities are neither attributable to Microsoft nor do they represent Microsoft's opinion. **b.** Microsoft shall only be liable if material obligations of the Agreement have been violated. **c.** Microsoft, its vicarious agents and/or its legal representatives shall not be liable for any indirect damage, including financial loss, such as loss of profit, unless Microsoft, its vicarious agents and/or its legal representative have at least acted with gross negligence or wilful misconduct. **d.** Any statutory no-fault liability of Microsoft, including statutory liability for breach of warranty, shall remain unaffected by the limitation of liability. The same shall apply to liability of Microsoft, its vicarious agents and/or its legal representatives in the event of fraud or their negligence resulting in personal injury or death. **e.** Microsoft is not responsible or liable for any failure to perform or delay in performing its obligations under these Terms to the extent that the failure or delay is caused by circumstances beyond Microsoft's reasonable control (such as labour disputes, acts of God, war or terrorist activity, malicious damage, accidents or compliance with any applicable law or government order). Microsoft will endeavour to minimise the effects of any of these events and to perform the obligations that aren't affected.
Norton Online Backup	"Some states and jurisdictions including member countries of the European Economic Area, do not allow for the limitation or exclusion of liability for incidental or consequential damages so the below limitation or exclusion may not apply to you. (a) To the maximum extent permissible under applicable law, you assume total responsibility for use and results of use of the service. Symantec and its licensors exercise no control over and disclaim any responsibility for the content or data created or accessible using the service. You agree not to use the service in high risk activities where an error could cause damage or injury. (b) To the maximum extent permissible under applicable law (…) Symantec, its licensors (…) will not be liable to you for any incidental, indirect, special, reliance, punitive or consequential damages of any kind (…) (d) Symantec and its licensors disclaim all liability or responsibility if service changes require changes to your equipment, degrade your equipment performance or service performance with the equipment, or make your equipment obsolete."
PayPal	"We shall only be liable to you for loss or damage caused directly and reasonably foreseeable by our breach of this Agreement and our liability in these circumstances is limited..."; Paypal further disclaims liability for "loss of profits, goodwill, business, contracts, revenue or anticipated savings (…) loss or corruption of data (…) loss or damage whatsoever which does not stem directly from our breach of this Agreement, (…) any loss or damage whatsoever which is in excess of that which was caused as a direct result of our breach of this Agreement (…) Nothing in this Agreement shall limit our liability resulting from our fraud or fraudulent misrepresentation, gross negligence, wilful misconduct, for death or personal injury resulting from either our or our subcontractor's negligence or to the extent such limitation or exclusion is not permitted by applicable law."

XIV. Section 4.3.3 – Monetary Limits

	Monetary Limits
500px	"to the extent the foregoing limitation of liability is prohibited or fails of its essential purpose, 500px' sole obligation to you for damages shall be limited to $100.00."
AWS	"in any case, our and our affiliates' and licensors' aggregate liability under this agreement will not exceed the amount you actually pay us under this agreement for the service that gave rise to the claim during the 12 months before the liability arose."
ADRIVE	"The total liability of Adrive (…) for any damage or claim arising from use of the services or the accompanying documentation shall not exceed the amount actually paid over the preceeding twelve (12) months by you for the software."
Basecamp	No information provided on monetary limits.
Datapipe	"Gogrid's liability arising out of or related to this agreement will not exceed the total amount of fees paid by customer during the 12 months preceding the injury giving rise to the claim."; in addition, in what service underperformance, the SLA establishes that the remedies indicated therein are the customer's sole and exclusive remedies for such.
Dropbox	"Other than for the types of liability we cannot limit by law (as described in this section), we limit our liability to you to the greater of $20 USD or 100% of any amount you've paid under your current service plan with Dropbox."
Facebook	"Our aggregate liability arising out of this statement or Facebook will not exceed the greater of one hundred dollars ($100) or the amount you have paid us in the past twelve months."
Google Drive	"The total liability of Google, and its suppliers and distributors, for any claims under these terms, including for any implied warranties, is limited to the amount you paid us to use the services (or, if the subject of the claim is the free service, to supplying you the services again)." **However**, "Nothing in these terms is intended to exclude or limit the liability of Google and its suppliers and distributors for death or personal injury, fraud, fraudulent misrepresentation or any liability that cannot be excluded by law."
iCloud	No information provided on monetary limits.
Instagram	"In no event will the Instagram parties total liability to you for all damages, losses or causes or action exceed one hundred united states dollars ($100.00)."
Linode	"Subscriber further acknowledges that Linode.com's liability for its own negligence may not in any event exceed an amount equivalent to charges payable by subscriber for services during the period damages occurred."
MEGA	"Despite the above, if any court or other competent authority holds us (…) liable for any matter related to these terms or our services, our total combined liability will be limited to the most recent subscription amount you have paid to us."
Microsoft OneDrive	No information provided on monetary limits.
Norton Online Backup	"(c) To the maximum extent permissible under applicable law (…) your exclusive remedies for such claim will be limited to the total charges paid by you to Symantec for the affected service in the one month immediately preceding the occurrence of the event giving rise to the claim. Symantec's total aggregate liability arising from or related to this agreement will not exceed the total charges paid by you to Symantec under this agreement in the one month immediately preceding the occurrence of the event giving rise to the claim."
PayPal	No information provided on monetary limits.

XV. Section 4.3.4 – Indemnification by the Customer/User

	Indemnification by the Customer/User
500px	"You hereby agree to indemnify and hold harmless 500px, its affiliated and associated companies (…) resulting from or arising out of (i) a breach of these Terms, (ii) Content posted on the Site, (iii) the use of the Services, by you or any person using your account or 500px Username and password, (iv) the sale or use of your Marketplace Images, or (v) any violation of any rights of a third party."
AWS	"You will defend, indemnify, and hold harmless us, our affiliates (…) from and against any Losses arising out of or relating to any third-party claim concerning: (a) your or any End Users' use of the Service Offerings (…); (b) breach of this Agreement or violation of applicable law by you, End Users, Your Content or Your Submissions; (…) (d) a dispute between you and any End User."
ADRIVE	"You agree to defend, indemnify and hold ADrive and its agents, employees, consultants, representatives and/or assignees harmless from and against any and all claims (…) relating to, arising out of or resulting from, in whole or in part, any acts or omissions by You, Your Storage Data…."
Basecamp	No information provided on indemnification by the customer/user, in its ToS.
Datapipe	"Customer will defend, indemnify, and hold harmless GoGrid (including its officers, directors, employees, agents, contractors, representatives, suppliers, subsidiaries, parents, affiliated companies, and insurers) from a third party claim, including without limitation a claim by any of Customer's customers or users, arising out or related to Customer's alleged or actual use of, misuse of, or failure to use the Services"
Dropbox	"The Customer will indemnify, defend and hold harmless Dropbox from and against all liabilities, damages and costs (including settlement costs and reasonable legal fees) arising out of any claim by a third party against Dropbox and its Affiliates."
Facebook	"If anyone brings a claim against us related to your actions, content or information on Facebook, you will indemnify and hold us harmless from and against all damages, losses, and expenses of any kind (including reasonable legal fees and costs) related to such claim."
Google Drive	Google Drive ToS does not provide anything; however, Google's general ToS indicates that "If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits, judgments, litigation costs and attorneys' fees."
iCloud	"You agree to defend, indemnify and hold Apple, its affiliates, subsidiaries, directors, officers, employees, agents, partners, contractors, and licensors harmless from any claim or demand, including reasonable attorneys' fees, made by a third party, relating to or arising from: (a) any Content you submit, post, transmit (…); (b) your use of the Service; (c) any violation by you of this Agreement; (d) any action taken by Apple as part of its investigation of a suspected violation of this Agreement or as a result of its finding or decision that a violation of this Agreement has occurred; or (e) your violation of any rights"
Instagram	"You (…) agree to defend (at Instagram's request), indemnify and hold the Instagram Parties harmless from and against any claims, liabilities, damages, losses, and expenses, including without limitation, reasonable attorney's fees and costs, arising out of or in any way connected with any of the following (including as a result of your direct activities on the Service or those conducted on your behalf)"
Linode	"Linode.com wishes to emphasize that in agreeing to the Linode.com Terms of Service, customer indemnifies Linode.com for any violation of the Terms of Service that results in loss to Linode.com or the bringing of any claim against Linode.com by any third-party. This means that if Linode.com is sued because of a customer's or a customer of a customer's activity, the customer will pay any damages awarded against Linode.com, plus all costs and reasonable attorney's fees."
MEGA	"You shall indemnify us against all claims, costs (including all our legal costs), expenses, demands or liability, damages and losses whether direct, indirect, consequential, or otherwise, and whether arising in contract, tort (including in each case negligence), or equity or otherwise, arising directly or indirectly from breach by you or anyone you give access to your data, of any of these terms or any policy referenced in these terms."
Microsoft OneDrive	No information provided on indemnification by the customer/user, in its ToS or in the Microsoft Services Agreement.
Norton Online Backup	"To the maximum amount permissible under applicable law, You shall indemnify and hold Symantec (…) harmless from and against any third party claims, demands, costs, damages, losses, liabilities and expenses, including reasonable attorneys' fees, made by any third party arising out of or in connection with use of the Service through Your Norton Account, including but not limited to liability arising out of or in connection with the Data transmitted or stored through the Service in connection with Your Norton Account."

PayPal	"You agree to defend, reimburse or compensate us (known in legal terms to "indemnify ") and hold PayPal, our other companies in our corporate group, the people who work for us or who are authorised to act on our behalf (including, without limitation, our service providers) harmless from any claim or demand (including legal fees) made or incurred by any third party due to or arising out of your or your employees' or agents' (or, where a third party otherwise acts on your behalf with your permission, that third party's) actions and/or inactions, breach of this Agreement, breach of any law, breach of the rights of a third party, use of your PayPal account and/or use of the Services, our infrastructure, our websites, our software and our systems (including any networks and servers used to provide any of the Services) operated by us or on our behalf."

XVI. Section 4.3.5 – SLAs and Service Credits

SLAs and Service Credits

500px	No information provided on SLAs or service credits.
AWS	AWS provides SLAs associated the use of its AWS services which include the provision of service credits, when availability falls beneath a certain point.[309]
ADRIVE	No information provided on SLAs or service credits.
Basecamp	Basecamp provides an SLA where it states that "for any given day where an outage exceeds 5 minutes, we'll credit your account 10x for a full hour that is equal to the hourly rate you pay us for use of Basecamp. (…) That is the full limit of our liability under this SLA."
Datapipe	Datapipe provides an SLA document, containing multiple metrics and their corresponding calculation. Datapipe claims that it will provide Customer with a 10,000% Service Credit for underperformance/unavailability, however, a number of additional limitation apply, namely that: "No credit will exceed one hundred percent (100%) of Customer's fees for the Service feature in question in the Customer's then-current billing month.", "The minimum period of Failure eligible for a credit is 15 minutes" (…) "The maximum credit during a single calendar year, for all Service features combined, is two months' Service fees, regardless of the length of Failure or the number of occurrences" and that "In the event that credits for any calendar month exceed 25% of GoGrid's revenues for such period, GoGrid may reduce and pro-rate the value of credits given to all Customers for such period so that the aggregate credit given to all Customers does not exceed 25% of revenues."
Dropbox	No information provided on SLAs or service credits.
Facebook	No information provided on SLAs or service credits.
Google Drive	No information provided on SLAs or service credits.
iCloud	No information provided on SLAs or service credits.
Instagram	No information provided on SLAs or service credits.
Linode	No specific SLA document, nonetheless "Linode.com provides a 99.9% uptime guarantee on all Linode hardware, and on network connectivity. In any given month, if your Linode is down for more than 0.1%, you may request a pro-rated credit for the down-time."
MEGA	No information provided on SLAs or service credits.
Microsoft OneDrive	No information provided on SLAs or service credits.
Norton Online	No information provided on SLAs or service credits.

[309] See https://aws.amazon.com/compute/sla/.

Backup	
PayPal	No information provided on SLAs or service credits.