RE-THINKING THE ALLOCATION OF ROLES UNDER THE GDPR IN THE CONTEXT OF CLOUD COMPUTING

SUMMARY

- *Cloud computing is a well-established and flourishing phenomenon, whose key activity on personal data is the storage thereof. This study analyses the allocation of the controller-processor roles under the GDPR to the cloud computing actors in the context of the storage of personal data. It examines the current controller-processor model and suggests a joint controllership interpretation to the EU regulators, as a more appropriate allocation of roles in the context of cloud computing.*
- *We argue that the prevailing controller-processor interpretation stems from the current primacy of the purpose criterion, as well as the recognition of consent as a criterion to allocate controllership. This article suggests that cloud providers control some of the essential means of the storage of personal data, thereby shifting part of the control from cloud customers to cloud providers.*
- *If the joint controllership approach was to be followed by the EU regulators, this article argues that it would better reflect the economic and technical reality, and provide a more appropriate responsibility and liability framework for cloud providers and customers, which in turn would enhance the level of protection that data subjects should benefit from under the GDPR.*

KEYWORDS:

Cloud computing; Consent; GDPR; Joint controller; Means; Purpose

INTRODUCTION

Estimates reveal a trend of exponential growth of data volume: compared to 2018, the European Commission expects a 530% increase thereof by 2025.[1] Such colossal quantities of data naturally require sophisticated technologies for their processing and use (in which case artificial intelligence will be an instrumental technology), as well as for their storage. It is specifically in the context of storing data that cloud computing - viewed as the 'backbone of the Internet'[2] - plays a key role.[3]

Cloud computing can, in essence, be defined as the delivery of computing resources via the Internet.[4] The development of cloud computing has had the effect of liberating users of computing resources from the burden of purchasing or building as well as managing these resources they do not often use to their full potential. With the advent of cloud computing, users of computing resources were able to purchase services delivered by a third party that owns, manages, and provides computing resources. This ultimately allows users to focus on their core activities.[5]

Aim of the Research

One of the most salient legal challenges relative to cloud computing pertains to data security and compliance, in particular privacy and data protection.[6] For the purpose of achieving the level of data

[1] Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region: A European strategy for data' (Communication) COM(2020) 66 final.

[2] Joris van Hoboken and others, 'Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape' (European Commission, 2019) 10 < https://data.europa.eu/doi/10.2759/284542 > accessed 2 December 2022.

[3] Commission, 'Commission Staff Working Document: Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' SWD(2022) 34 final.

[4] Sandeep Bhowmik, *Cloud Computing* (CUP 2017) 2. See also Peter Mell and Tim Grance, 'The NIST Definition of Cloud Computing' (Special Publication 800- 145, National Institute of Standards and Technology, US Department of Commerce 2011) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> accessed 19 October 2022 where the National Institute of Standards and Technology (NIST) proposed a definition that is still widely accepted and recognised today: 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.' See also the definition enshrined in Article 4(19) of the 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 [2016], OJ L194/1 (NIS Directive): 'cloud computing service means a digital service that enables access to a scalable and elastic pool of shareable computing resources'. Recital 17 of the NIS Directive further explains the definition of Article 4(19). Finally, in Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022], OJ L333/80 (NIS 2 Directive), we can find a slightly different definition, focusing on the on-demand and distributed features of cloud computing. Thus, Article 6(30) of the NIS 2 Directive defines a cloud computing service as 'a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations'.

[5] Dan C Marinescu, *Cloud Computing: Theory and Practice* (3rd edn, Morgan Kaufmann 2022) 2.

[6] Bhowmik (n 4) 38.

protection warranted by the General Data Protection Regulation[7] ('GDPR'), it is paramount to properly designate the entity responsible for the compliance with data protection obligations enshrined in this instrument. The standard view has been that cloud providers should be qualified as 'processors' under the GDPR, whereas cloud customers (as natural or legal persons) are deemed 'controllers' (see below). This article revisits this controller-processor paradigm and aims at recommending to the EU regulators (EDPB[8] and EDPS[9]) a joint controllership interpretation for the storage of personal data in the cloud computing context. This recommendation will be supported by two main arguments: first, the current paradigm fails to accommodate the requirement whereby the controller must determine the essential means of the data processing activity; second, it leads to undesirable consequences, both for the cloud customers and the data subjects.

Cloud Computing: Definition and Scope of the Research

To conduct the analysis related to the (more adequate) distribution of roles between cloud providers and cloud customers under the GDPR, it is necessary to clarify certain conceptual aspects relative to cloud computing. Three layers of computing resources can be delivered via the Internet, namely the infrastructure layer, the platform layer, and the application layer.[10] This taxonomy corresponds to the three service models of cloud computing: Infrastructure as a Service ('IaaS'), Platform as a Service ('PaaS'), and Software as a Service ('SaaS').

First, the IaaS model is characterized by the fact that the provider offers an infrastructure as a service to its customer. That infrastructure includes physical components (or hardware), such as a processor, memory, network, or storage devices.[11] Amazon S3 as a storage service constitutes a telling example of the IaaS model.[12]

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L119/1.

[8] 'EDPB' stands for European Data Protection Board.

[9] 'EDPS' stands for European Data Protection Supervisor.

[10] Bhowmik (n 4) 6.

[11] *ibid*.

[12] Bhowmik (n 4) 79.

Second, under the PaaS model, the provider offers the platform, *i.e.* the layer composed of both hardware and software components that allow customers to install, develop, or run applications.[13] Examples of PaaS include Microsoft Azure, Google Apps, Force.com.[14]

Third, the cloud customer can directly access a software or application (*e.g.* ERP[15], CRM[16] or social networks) that is running on a computing architecture managed by the cloud provider. Thus, the cloud customer does not need to install or configure the application; the latter is simply accessible on the Internet.[17] Examples of SaaS include YouTube, Gmail, Google Docs, and Google Calendar.[18]

In addition to the taxonomy based on the three cited service models, there is another, deployment-based taxonomy, which includes private, community, public, and hybrid clouds. The distinguishing feature of a private cloud is that the cloud infrastructure is only used by a single entity. Alternatively, a public cloud is accessible by the general public and because of this, is necessarily hosted off the premises of the cloud customer, and on the premises of the cloud provider. A so-called community cloud is a cloud that is provisioned and used by a closed community, while a hybrid cloud is a combination of two or more of the abovementioned deployment models.[19]

In this article, we only focus on public clouds because they are the most widespread deployment model and the one that generally comes to mind when thinking about the cloud.[20] In addition, it is public clouds that pose the most serious challenge to the prevailing controller-processor interpretation, as they are more standardised and lead to a greater shift of control from the cloud customer to the cloud provider.[21]

Through these service and deployment models, a vast array of services can be delivered, including those

[13] Bhowmik (n 4) 6, 79; Marinescu (n 5) 15-16.

[14] Marinescu (n 5) 34.

[15] 'ERP' stands for Enterprise Resource Planning.

[16] 'CRM' stands for Customer Relationship Management.

[17] Bhowmik (n 4) 80; Marinescu (n 5) 15.

[18] Marinescu (n 5) 34.

[19] Mell and Grance (n 4) 3; Fang Liu and others, 'NIST Cloud Computing Reference Architecture' (Special Publication 500-292, National Institute of Standards and Technology, US Department of Commerce 2011) 10-12 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf> accessed 7 December 2022.

[20] Flexera, 'State of the Cloud Report 2020' (2020) <https://info.flexera.com/SLO-CM-REPORT-State-ofthe-Cloud-2020> accessed 7 December 2022.

[21] Marinescu (n 5) 265. See also Ronald Leenes, 'Who Controls the Cloud?' (2010) 11 IDP : revista de internet, derecho y política 1, 3.

concerning personal data. In this article, we only address the processing activity consisting of the storage of personal data, as well as the activities that are ancillary thereto (such as the duplication or replication of the data, the deletion thereof, and their securing).

It goes without saying that addressing any type of data processing activity that can be pursued in the context of the cloud (*e.g.* performance monitoring, AI analytics, predictive maintenance, detection of fraud, data conversion or curation, generation of reports, etc) would be extremely difficult, inasmuch as those activities vary from contract to contract. In light of this, we will focus on the most important and common of those activities, *i.e.* the storing of personal data. It should also be stressed that, in this article, we do not analyse the data processing activities pursued by the cloud providers alone, *i.e.* for their own purposes because in this case, the cloud provider's quality as an independent controller is beyond doubt.[22]

Structure of the Research

This article will, first, revisit and critically assess the current controller-processor interpretation in the context of cloud computing (Section 1). We begin our analysis with an account of the concepts of (joint) controllers and processors under the GDPR, as well as their current application - and the rationale therefor - in the context of cloud computing. Based on that analysis, we then present four key reasons to nuance and possibly revise the current interpretation. It results from these reasons that, contrary to what the controller-processor interpretation would mandate, the cloud customer has no decision-making power over all elements (or means) it is presumed to control under the current interpretation. Additionally, we claim that the controller-processor interpretation leads to undesirable consequences, both for the cloud customers and the data subjects. These consequences concern in particular the lack of fairness for the cloud customer and the loss of control for the data subjects.

We will secondly argue in favour of the interpretation of the cloud computing actors by the EU regulators as joint controllers (Section 2). Based on this proposition, we will outline the effects of joint controllership for cloud providers, cloud customers, as well as data subjects, and argue, in our

[22] European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (7 July 2021, Version 2.1) para 81.

concluding remarks, that the joint controllership qualification would lead to a fairer distribution of responsibilities and liabilities amongst cloud providers and cloud customers, ultimately enhancing the level of protection that data subjects should benefit from under the GDPR.

I. CRITICISMS OF THE PREVAILING VIEW

Prevailing View

1. Key concepts

The GDPR's personal scope of application is focused on two main types of actors, controllers and processors.[23] The controller is defined in Article 4(7) of the GDPR as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. When several entities act as controllers for the same data processing activity, they are qualified as 'joint controllers'. The processor is defined in Article 4(8) of the GDPR as the 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

The key difficulty in allocating the roles (controller and processor) is the correct designation of the entity that concretely[24] determines the purposes and the means of the data processing activity.[25] The 'purposes' refer to the *why* of the data processing activity, *i.e.* to the outcome pursued by the controller. The 'means' refer to the *how* of the data processing activity. The EDPB suggested a distinction between two kinds of means that is, 'essential' and 'non-essential'.[26] So-called 'essential' means are considered closely intertwined with the purpose, as they define the key parameters of the data processing activity, *i.e.* the type of personal data processed, the duration of the processing, the categories of recipients and the categories of data subjects. The so-called 'non-essential' means pertain to more practical aspects, such

[23] For a detailed description of the concepts of controller and processor, please see European Data Protection Board, 'Guidelines 07/2020' (n 22).

[24] The GDPR adopts a functional definition of controllers and processors. See European Data Protection Board, 'Guidelines 07/2020' (n 22) para 12.

[25] In its guidelines, the EDPB clarifies that the test must be performed at the level of each processing activity. See European Data Protection Board, 'Guidelines 07/2020' (n 22) para 26.

[26] European Data Protection Board, 'Guidelines 07/2020' (n 22) 15-16.

as the type of hardware or software or the detailed security measures.[27] Even though the processor may influence the non-essential means, only the controller has a decision-making power over the essential means.[28]

If controllers jointly determine the purposes and the means, they are joint controllers as per Article 4(7) of the GDPR. This joint determination can result from a common decision or converging decisions. On the one hand, the common decision is the classic example of joint controllership where two or more controllers are bound by a common intention and decide together on the purposes as well as the means. On the other hand, decisions are considered to be converging if they 'complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing'.[29] This convergence occurs if 'the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, *i.e.* inextricably linked'.[30] Joint controllers do not need to exercise the same influence but can be involved to varying degrees, as well as at different stages.[31] The Court of Justice of the European Union ('CJEU') also shed some light on the elements that are relevant for qualifying an entity as controller. In the landmark *Google Spain* case, the Court ruled that Google's knowledge of whether personal data were processed was not a relevant criterion to determine if Google was, indeed, processing personal data.[32] It follows from this case that the (absence of) knowledge of the quality of the processed data (personal or not) is not relevant to confer the quality of controller.[33] The CJEU also added that the lack of control over the personal data would not prevent the qualification as controller.[34] In that context, the CJEU subsequently made clear that being a controller does not require

[27] *ibid* para 40.

[28] *ibid* para 40.

[29] *ibid* para 55.

[30] *ibid* para 55.

[31] Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] ECLI:EU:C:2018:388, para 43. This has been confirmed in Case C-25/17 *Jehovan todistajat* [2018] ECLI:EU:C:2018:551, para 66 and Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629, para 70. See also European Data Protection Board, 'Guidelines 07/2020' (n 22) paras 58 and 63.

[32] Case C-131/12 *Google Spain and Google* [2014] ECLI:EU:C:2014:317, para 28.

[33] Michèle Finck, 'Cobwebs of Control: the Two Imaginations of the Data Controller in EU Law' (2021) 11(4) International Data Privacy Law 333, 335.

[34] *Google Spain* (n 32) para 34.

actual access to personal data.[35]

In the following section, we will show how the concepts of (joint) controllers and processors have been applied in the context of cloud computing.

2. Current interpretation of these concepts in the cloud environment

In its opinion on Cloud Computing from 2012, the Article 29 Data Protection Working Party (the 'WP29', the predecessor of the EDPB) explicitly qualified cloud providers as processors, and cloud customers as controllers.[36] This qualification focused directly on why a given processing activity was occurring, *i.e.* who was at the initiative of the processing of personal data. Following this method, the cloud customer assumes the role of controller under the GDPR. The WP29 justified this view by the fact that 'the cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation'.[37] Alternatively, the WP29 provided very little explanation on the rationale of qualifying the cloud provider as a processor: 'When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor'.[38]

The WP29 thus gave the 'canonical' reading of 'controller' and 'processor' in the context of cloud computing which has shaped the majority view on the matter since 2012. The EDPB confirmed the WP29's approach in its 2020 guidelines, which reassert on the one hand that a cloud customer ought to qualify as controller because it decides 'to make use of this particular cloud service provider in order to process personal data for its purposes'[39] and on the other hand that a cloud provider ought to qualify as processor, namely because the cloud provider does not know whether the data it hosts - deemed encrypted - are personal or not.[40] In its 2023 report on the use of the cloud by the public sector, the

[35] *Wirtschaftsakademie* (n 31) para 38. This has been confirmed in *Jehovan* (n 31) para 69 and in *Fashion ID* (n 31) para 69.

[36] Article 29 Working Party, 'Opinion 05/2012 on Cloud Computing' (WP 196, 1 July 2012) 7-8.

[37] *ibid* 7.

[38] *ibid* 8.

[39] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 30.

[40] *ibid* para 40. In that regard, the CJEU of Justice has explicitly rejected the (absence of) knowledge about the type of data (personal or not) as a criterion in the *Google Spain* case. See *Google Spain* (n 32) para 28. See also in that respect Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019) para 1206.

EDPB fully confirmed its standpoint on the qualification of the cloud actors.[41]

The prevailing view on the allocation of the controller-processor roles in the context of cloud computing was also supported by part of legal scholarship. Some have considered that the cloud provider assumes a passive role, limited to only providing computing resources.[42] They have also suggested that the fact that it is the cloud customer that selects the cloud provider[43] and the specific cloud service[44] plays a determining role in the qualification of the cloud customer as controller.

3. Purposes and consent as the defining criteria

It follows from the above that the defining criterion for the current controller-processor interpretation was the choice made by the cloud customer at the origin of the relationship. This fact underlies the entire set of responsibilities - the inobservance of which is sanctioned by potentially severe sanctions - enshrined in the GDPR.[45]

The emphasis put on the initiative of the cloud customer reflects a general trend to view as more important the 'why' of the data processing activity (*i.e.* the purposes), undermining the importance of the means through which that processing is conducted.[46] This is open to criticism if we consider the wording, the history and the purposes of the GDPR. Taken literally, Article 4(7) places the purposes and the means on equal footing.[47] It is true that in the drafting of the GDPR, the question did arise as to whether the capacity to define the means of data processing should be a criterion to define controllership. Evidently, the EU legislature chose to maintain the means as a definitional element of the quality of controller.[48] In addition, the means criterion is aligned with the functional approach followed in the GDPR, which consists in qualifying as controllers the entities that exercise actual and factual influence

[41] European Data Protection Board, '2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector' (17 January 2023) footnotes 21 and 30.

[42] Dimitra Kamarinou, Christopher Millard and Felicity Turton, 'Responsibilities of Controllers and Processors of Personal Data in Clouds' in Christopher Millard (ed), *Cloud Computing Law* (2nd edn, OUP 2021) 300; W Kuan Hon, Christopher Millard and Jatinder Singh, 'Control, Security, and Risk in the Cloud' in Christopher Millard (ed), *Cloud Computing Law* (2nd edn, OUP 2021) 31-33.

[43] Kamarinou, Millard and Turton (n 42) 300.

[44] Van Alsenoy (n 40) 479.

[45] See also Finck (n 33) 335 and 346.

[46] Van Alsenoy (n 40) para 694; Finck (n 33) 334.

[47] *ibid*.

[48] Van Alsenoy (n 40) para 695.

over the processing.[49] This approach is also employed in the responsibility and liability context: controllers must fulfil obligations and may potentially be liable as a consequence of their factual influence, *i.e.* because they are able to ensure the compliance with the GDPR.[50]

Moreover, in the context of unilaterally drafted contracts and terms of business, the EDPB went one step further in the distance it took with the GDPR, stressing that:

> [T]he imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR.[51]

It can be inferred from this statement that the key element in defining controllership and allocating the responsibilities associated with it, is the consent given to a provider. This is not a novel idea. Scholars like Léonard and Mention[52] have considered the indirect determination of the purpose and means via a consent mechanism. The CJEU seems to also have endorsed this view. The Court stressed that the 'knowledge'[53] and the status of the controller as 'fully aware'[54] of a data processing activity are relevant factors to identify the locus of controllership. In a similar vein, in *Fashion ID*, the CJEU implied that having 'consented (…) in order to benefit from the commercial advantage' would satisfy the formal criterion of determining the purpose of the data processing activity.

However, regulators have not yet explicitly acknowledged that consent is, or ought to be a formal criterion to identify controllers. As already mentioned, this is no doubt due to the prevailing functional

[49] *ibid* para 1369.

[50] *ibid* paras 1223, 1265 and 1284.

[51] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 110.

[52] Thierry Léonard and Anthony Mention, 'Transferts transfrontaliers de données: quelques considérations théorique et pratiques', in Benjamin Docquir and Andrée Puttemans (eds), *Actualités du droit de la vie privée* (Bruylant 2008) 105. See also footnotes 43 and 44 above for scholars considering that cloud customers qualify as controllers because they select the cloud provider and/or service. In our view, these scholars indirectly allude to the legal concept of 'consent' without naming it, overlooking thereby the requirements of a legally valid consent. In this respect, we refer in particular to the section below on power asymmetry.

[53] *Jehovan* (n 31) para 71.

[54] *Fashion ID* (n 31) para 77.

approach that is followed in the allocation of roles, obligations and liability under the GDPR.

Besides, if the EU regulator were to consider consent as a valid requirement for the definition of controllership, practitioners would need to examine the circumstances under which that consent was given in order to be considered free and informed. We will show, in the remainder of this article[55], that those requirements can be challenged.

At this stage, may it suffice stressing that, because of the current primacy of the purpose criterion and the potential recognition of consent as a criterion, little attention has been paid to the determination of the essential means of the storage of personal data in the context of cloud computing. As we will argue, a proper consideration of the means would challenge the prevailing controller-processor interpretation. In our view, identifying the entity displaying the concrete ability to protect the personal data of data subjects and take preventive actions against potential infringements would bring the qualification of the cloud actors in line with the literal, historic and teleological interpretation of the controller concept. In other words, as originally contemplated by the EU lawmaker, responsibilities should be allocated to the entity having a decision-making power over the essential means or, as Finck puts it, over the 'techno-organizational structure' of the data processing activity.[56]

Critical Analysis of the Prevailing View Based on the Reality of the Cloud

There are four concrete reasons why the prevailing interpretation can and even should be revisited: (1) the cloud provider controls the underlying infrastructure, (2) the very purpose of the cloud customer relying on externalised services is to be released from certain responsibilities, (3) the power asymmetry between the cloud provider and the cloud customer prevents the cloud customer from being the sole controller, and (4) the evolution of the EU's regulatory landscape tends to shift responsibilities towards cloud providers.

1. Control of the underlying infrastructure

In the context of cloud computing, most computing resources are in fact controlled and managed by

[55] See mainly the section on power asymmetry.

[56] Finck (n 33) 334.

cloud providers.[57] As a result, cloud customers have very little control over the computing environment.[58] Indeed, cloud providers control at the very least the underlying physical computing resources, such as computers (CPU and memory), networks and storage components.[59] In the case of IaaS, the cloud provider solely controls the underlying physical infrastructure, as well as the abstraction level.[60] In the case of PaaS, the cloud provider also controls the platform layer, and in the case of SaaS, the cloud provider controls all layers. The degree of control largely depends on the type of model, with the IaaS offering more control to cloud customers, and the SaaS offering the least control.[61] [62]

As the physical resources are managed and controlled by the cloud provider, cloud customers cannot access the physical resources (hardware).[63] These physical resources are always managed and controlled by the cloud provider and made accessible in a virtualised way to the cloud customer via the Internet.[64] This has consequences in terms of the control over the data which, through cloud computing, is largely shifted towards the cloud provider.[65] Engineer and Computer Scientist Sandeep Bhowmik goes so far as to say that 'cloud computing companies have total control over those data stored in their data centres. How they use those sensitive data depends on their moral'.[66] Cloud customers' lack of operational control over data is also recognised by the European Commission.[67] The WP29 was already aware of the loss of control caused by the use of the cloud in 2012, but it considered this a risk of the cloud, rather than a relevant criterion to qualify the actors of cloud computing.[68]

---

[57] Liu and others (n 19) 7; Article 29 Working Party, 'Opinion 05/2012' (n 36) 5; Bhowmik (n 4) 47-48, 68, 78, 330.

[58] Liu and others (n 19) 7, 87, 98; Bhowmik (n 4) 47; Marinescu (n 5) 8.

[59] Liu and others (n 19) 13.

[60] Bhowmik (n 4) 275.

[61] Knud Brandis, Srdan Dzombeta and Knut Haufe, 'Towards a Framework for Governance Architecture Management in Cloud Environments: A Semantic Perspective' (2014) 32 Future Generation Computer Systems 274, 278; W Kuan Hon, Christopher Millard and Jatinder Singh, 'Cloud Technologies and Services' in Christopher Millard (ed), *Cloud Computing Law* (2nd edn, OUP 2021) 6-7; Marinescu (n 5) 34.

[62] The type of deployment, *i.e.* private, community, public or hybrid also entails different degrees of control. Public clouds generally tend to offer less control to users, whereas private clouds offer more control. As our contribution is limited to public clouds, for more information, please see Bhowmik (n 4) 66-69; Hon, Millard and Singh, 'Cloud Technologies and Services' (n 61) 25.

[63] Bhowmik (n 4) 78.

[64] *ibid*.

[65] *ibid* 273; Marinescu (n 5) 1, 265. See also Francoise Gilbert, 'Cloud Service Providers as Joint-Data Controllers' (2011) 15(2) Journal of Internet Law 3, 3.

[66] Bhowmik (n 4) 48.

[67] SWD(2022) 34 (n 3) 27.

[68] Article 29 Working Party, 'Opinion 05/2012' (n 36) 5.

Even though platforms like Amazon commit to not accessing their customers' personal data, they may explicitly state that they are able to do so.[69] In the same vein, Dropbox is known for its 'cybertips', *i.e.* reports sent by Dropbox to the National Center for Missing & Exploited Children in cases where following a screening of the content uploaded by its users, Dropbox notices unlawful pornographic content.[70]

It follows that in actuality, the current 'controller' (*i.e.* the cloud customer) does not exercise much control over the data stored in the cloud. The cloud provider however does. At the very least, the cloud provider and the cloud customer share the control over the data. This conceptual or semantic discrepancy alone does not suffice to qualify cloud providers as controllers, especially since the operational access to the data is not a formal criterion to operate that qualification.[71] However, we argue that the cloud provider's control of the underlying infrastructure, coupled with the three other reasons discussed below, entails a determining degree of control over the essential means of processing.

2. Purpose of the cloud: cloud customers as users

As explained above, the cloud computing model removes from the cloud customers the burden of managing the computer resources, since the management is performed by the cloud provider.[72] As Bhowmik puts it, cloud customers 'will simply use [the computing resources] without the responsibility of managing [them]'.[73] In addition, gaining more control over the computing resources will often entail increasing costs for the cloud customer, so that the latter may be reluctant to obtain more 'ownership' over the computing resources.[74]

Therefore, the current controller-processor view creates a strong discrepancy between the economic and

[69] Amazon, 'AWS Customer Agreement' <https://aws.amazon.com/agreement/> accessed 15 October 2022.

[70] See also Dropbox Terms of Services (Dropbox, 'Dropbox Terms of Service' <https://www.dropbox.com/terms> accessed 19 October 2022) and Acceptable Use Policy (Dropbox, 'Dropbox Acceptable Use Policy' <https://www.dropbox.com/acceptable_use> accessed 19 October 2022), clearly stipulating that Dropbox may review the content of its users to ensure that its users comply with the applicable legislation.

[71] *Wirtschaftsakademie* (n 31) para 38; *Jehovan* (n 31) para 69; *Fashion ID* (n 31) para 69. See also *Google Spain* (n 32) para 34. See also European Data Protection Board, 'Guidelines 07/2020' (n 22) para 45.

[72] Mell and Grance (n 4); Marinescu (n 5) 1. See also Commission, 'European Commission Cloud Strategy: Cloud as an enabler for the European Commission Digital Strategy' (16 May 2019) 5 < https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf> accessed 25 November 2022.

[73] Bhowmik (n 4) 57.

[74] *ibid* 330.

technological model of cloud computing on the one hand and the current legal paradigm on the other hand. While in practice, cloud customers often seek to take on a user role, the GDPR, as currently interpreted by the EDPB in connection to cloud computing, would mandate that cloud customers are actually responsible for (demonstrating) the protection of data subjects' data. This means that cloud customers must give clear instructions to the cloud provider about the processing of personal data to ensure that the cloud provider abides by the GDPR, as well as supervise the processing by the cloud provider, including, as the case may be, through audits on the cloud provider.[75] These instructions must address the permissibility to perform transfers of personal data to a third country or an international organisation, as well as, at the very least, the security objectives (that must be appropriate given the risk assessment performed by the controller).[76] In addition, the controller must accept the main security measures - including the changes thereto - that may be proposed by the processor.[77] The controller must also have the ability to consent or object to the use of sub-processors. Furthermore, they must review the information provided by the processor on among others the functioning of the systems used, the security measures, retention and location of data, transfers and recipients of data, as well as sub-processors and access to data.[78]

It follows that, as the GDPR opts for so-called 'functional' concepts, *i.e.* concepts that derive from concrete operations or actual facts[79], the mismatch discussed above should be taken into account in order to properly allocate the roles prescribed by the GDPR to the actors of the cloud.

3. Power asymmetry

Due to the size and expertise of cloud providers, they generally dictate their terms (such as the terms and conditions, terms of use and, most importantly in this context, data processing agreements) to their counterparts, even if the latter is also a (large) company.[80] Those terms are often non-negotiable, let

[75] European Data Protection Board, 'Guidelines 07/2020' (n 22) 35.

[76] *ibid* 36-37.

[77] *ibid* 37.

[78] *ibid* para 143.

[79] *ibid* para 12.

[80] Liu and others (n 19) 5; Gilbert (n 65) 3; Commission Nationale de l'Informatique et des Libertés, 'Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing' 5-6

alone imposed on certain aspects by the cloud customer to the cloud provider. The Digital Markets Act has clearly recognised this phenomenon, as it associates cloud computing services with their 'weak contestability' (see among others Recitals 13 and 14).[81] [82] In addition to the power asymmetry, cloud providers generally have a vast array of clients using their computing resources, and even sharing the same computing resources (what is called 'multi-tenancy'), so that cloud providers could simply not observe the (potentially conflicting) instructions from their customers.[83] Moreover, due to their often large client base, cloud providers cannot individually negotiate their contracts. Contracts with cloud providers are thus generally concluded via automatic means.[84] The inability of cloud providers to respect the instructions (if any) of their customers is further reinforced by the fact that, due to their frequent reliance on subcontractors, implementing the instructions of their customers would create the need to adapt the contractual framework with their subcontractors. This would simply prove to be impossible, due to their large number of customers. Due to these factors, the services are generally offered on a 'take it or leave it' basis.[85]

Concretely, cloud providers unilaterally determine the location of their data centres. Most often, cloud customers do not know where the data centres are located and have little - if any - knowledge of where their data are stored and backed up.[86]

In addition, cloud providers also possess a decision-making power over the subcontractor (or, in the data protection context, the 'sub-processor') they rely on[87], the persons that can access the data (access

<https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf> accessed 1 December 2022; Article 29 Working Party, 'Opinion 05/2012' (n 36) 8; Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region: Unleashing the Potential of Cloud Computing in Europe' (Communication) COM(2012) 529 final 11; Bhowmik (n 4) 47; Van Alsenoy (n 40) 480; Christopher Millard and others, 'At this Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9(4) International Data Privacy Law 217, 218; Kamarinou, Millard and Turton (n 42) 312, 337; SWD(2022) 34 (n 3).

[81] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022], OJ L265/1 (Digital Markets Act).

[82] The above-mentioned criticisms, and in particular the lack of control (or ownership) on the customer's data as well as the consequences of the power asymmetry have been spotted, sometimes in order to propose alternative technological or business solutions. In that respect, see mainly the Gaix-X project.

[83] Kamarinou, Millard and Turton (n 42) 312.

[84] Gilbert (n 65) 4.

[85] Hon, Millard and Singh, 'Cloud Technologies and Services' (n 61) 24.

[86] Hon, Millard and Singh, 'Cloud Technologies and Services' (n 61) 12-13; Bhowmik (n 4) 47, 49, 98, 296; Marinescu (n 5) 9, 265, 271. See also Benjamin Docquir, 'Le "Cloud Computing" ou l'Informatique Dématérialisée : la Protection des Données au Coeur de la Relation Contractuelle' (2011) 10 RDC 1000, 1010.

[87] Article 29 Working Party, 'Opinion 05/2012' (n 36) 6; Hon, Millard and Singh, 'Cloud Technologies and Services' (n 61) 18.

control[88]) and the security measures they implement.[89] It should be stressed that cloud providers generally adopt their own data duplication and retention policies so that cloud customers continue to have no knowledge of or control over the effective deletion of the data.[90]

It follows that cloud customers are precluded from giving instructions to cloud providers, as is required by the GDPR. Moreover, cloud customers are hardly able to 'request changes' about the services defined by the provider.[91]

In conclusion, the current controller-processor qualification leads to a situation where cloud customers, qualified as controllers, are unable to fulfil their obligations pursuant to the GDPR. Contrary to the EDPB[92], the EDPS has endorsed this conclusion, stating that the level of discretion whereby a party can unilaterally change contractual documents (and with that, the data processing purposes or location) renders this party a controller.[93] Finally, the professional expertise of an entity is another key criterion to identify the controller.[94]

4. Paradigm shift towards more regulatory responsibilities for cloud providers

In recent years, the EU lawmaker has gradually increased the responsibilities that apply to cloud providers in the context of the processing of personal data. In that connection, the NIS Directive[95] imposes security and notification requirements to, among others, cloud computing services.[96] These obligations are reinforced in the so-called NIS 2 Directive.[97] Even though these Directives do not apply

[88] Bhowmik (n 4) 98, 296.

[89] Commission Nationale de l'Informatique et des Libertés (n 80) 6; Van Alsenoy (n 40) para 1049; Marinescu (n 5) 5. See also Docquir (n 86) para 37.

[90] Bhowmik (n 4) 296; Hon, Millard and Singh, 'Cloud Technologies and Services' (n 61) 12; Marinescu (n 5) 258, 265. See also Docquir (n 86) para 1010.

[91] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 30.

[92] *ibid* paras 108 and 110.

[93] European Data Protection Supervisor, 'EDPS Public Paper on outcome of own-initiative investigation into EU institutions' use of Microsoft products and services' (2 July 2020) 9 <https://edps.europa.eu/data-protection/our-work/publications/papers/outcome-own-initiative-investigation-eu-institutions_en> accessed 26 October 2022.

[94] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 27.

[95] 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 [2016], OJ L194/1 (NIS Directive).

[96] See Article 4(5) in combination with Annex III, read in conjunction with Article 16 of the NIS Directive (n 95).

[97] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022], OJ L333/80 (NIS 2 Directive).

to personal data, they apply to systems that may host personal data, which means that the protection of personal data is indirectly ensured via these instruments.

In addition, the Data Act Proposal[98] intends to create new obligations for cloud providers to the extent that it aims among others at facilitating the interoperability of cloud services and thus at allowing the portability of data.[99] In the context of the Data Act Proposal, it is also interesting to observe the terms of Recitals[100] 21 and 24. These Recitals shed light on Chapter II of the Data Act Proposal, the goal of which, in a nutshell, is to give users of IoT products a right (and create the corresponding obligation for data holders) to access the data they generate through their use of such products. Recital 21 clarifies that the product data may be stored on-device or on a remote server. In the latter case, the server may be provided by a cloud provider which, according to Recital 21, would act as data holder. Recital 24, which comments on the interplay between the GDPR and the Data Act Proposal, adds that data holders would qualify as controllers under the GDPR. In short, the Recitals of the Data Act Proposal suggest that cloud providers would qualify as controllers. This poses yet another challenge to the prevailing controller-processor view.

In the same vein as the Data Act Proposal, the Digital Markets Act[101] also aspires to facilitate data portability, among others from a cloud provider qualifying as 'gatekeeper'[102].[103] It also limits and mandates certain data processing activities (*cf.* Articles 5.2, 6.2, 6.8, 6.10 and 7.8).

Contrary to the Free flow of non-personal data Regulation[104] that also aimed at favouring the porting of data, the NIS directive (as well as the NIS 2 Directive), the Data Act Proposal[105] and the Digital Markets

[98] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM(2022) 68 final (Data Act Proposal).

[99] See Article 2(12) in combination with Recitals 69, 76 and 79 read in conjunction with Chapters VI (Switching between data processing services) and VIII (Interoperability) of the Data Act Proposal.

[100] Although Recitals offer interpretations of the legal provisions enshrined in the main body of the Data Act Proposal, it should be noted that they are not binding.

[101] Digital Markets Act (n 81).

[102] The Digital Markets Act defines gatekeepers in its Article 2(1), which refers to Article 3 to specify the criteria that would qualify an undertaking as gatekeeper.

[103] See Article 2(2)(i) read in conjunction with Article 6.9 of the Digital Markets Act.

[104] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018], OJ L303/59.

[105] See Recital 7 and Article 1.3 explicitly stating that the Data Act complements the GDPR.

Act[106] do not exclude personal data from their material scope and, concerning the Data Act Proposal and the Digital Markets Act, they even mention that they complement the GDPR. These instruments can thus be employed to assess the qualification of cloud providers under the GDPR. Indeed, being bound by a legal obligation requiring the processing of personal data is a criterion to qualify an entity as controller. The GDPR - in the context of the definition of the controller in Article 4(7) - thus states that 'where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law'. As the EDPB puts it:

> [M]ore commonly, rather than directly appointing the controller or setting out the criteria for its appointment, the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task.[107]

Undesirable consequences of the prevailing view

In addition to our argument of inadequacy due to its non-correspondence to the reality of cloud computing, we further argue that the prevailing view - discussed above - yields undesirable effects. In the context of the relationship between the cloud provider and the cloud customer, the controller-processor interpretation leads to an erosion of the sense of responsibility on the part of the cloud provider. Indeed, at present, it is the cloud customer who bears the primary responsibility under the GDPR, while the cloud provider is considered a mere executor of the controller's instructions.[108] The erosion of cloud providers' sense of responsibility may, in turn, reduce the measures they would take to respect the GDPR and, consequently, increase their probability of violating the GDPR. Conversely, the cloud customer bears the primary responsibility for obligations it has no or little control over (*e.g.* the

[106] See Article 2(25) which defines personal data and Recital 59, which explicitly states that, with regard to the portability obligation, the Digital Markets Act complements the right to data portability as provided in the GDPR.

[107] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 24.

[108] Van Alsenoy (n 40) para 95.

security measures[109]), thereby disturbing the desired correlation between the liability framework and the ability to exert an influence over the respect of obligations.[110]

The prevailing view may, moreover, lead to a 'negative conflict of competence'[111], *i.e.* a situation where neither the cloud customer nor the cloud provider assumes responsibility for a particular obligation. This would be the case if the cloud provider did not bear the primary responsibility for an obligation, and if the cloud customer felt that they did not have the tangible control and power to fulfil that obligation. This responsibility loophole phenomenon is further reinforced by Article 28 of the GDPR, which lists the clauses that must be stipulated in the agreement between the controller and the processor. As a result, such agreements are generally standardised and not tailored to a specific situation at hand. Concretely, responsibilities are artificially allocated under Article 28 of the GDPR, and not based on the actual control controllers and processors exercise.[112] In addition, since the controller needs to be able to address data subjects' requests, it must at least have the control over the data or the ability to give instructions to its processors. In the case of cloud computing, the controller (the cloud customer) often lacks sufficient control over both of those elements, thereby hampering proper responses to data subjects' requests.

The alarming consequences of this are the negative externalities for the data subjects, as the central figure of the protective safeguards enshrined in the GDPR.[113] As per Articles 13(1)(e), 14(1)(e) and 15(1)(c) of the GDPR, in a controller-processor situation, data subjects only receive information about the (type of) entity receiving their personal data. They are not informed of the allocation of responsibilities between the controller and the recipient which means that the actual processing

[109] We address the allocation of responsibilities for the security measures in more detail under the Section below entitled 'Allocation of responsibilities between the joint controllers'. At this stage, it is sufficient to note that, while the security of personal data is a shared responsibility between the cloud provider and the cloud customer, the cloud provider often defines the basic security measures. In addition, the cloud provider's level of control increases with the type of cloud model: from IaaS (with the least control over the security measures by the cloud provider) to SaaS (with the highest level of control by the cloud provider).

[110] Yordanka Ivanova, 'Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020) 15; Benjamin Wong, 'Problems with Controller-Based Responsibility in EU Data Protection Law' (2021) 11(4) International Data Privacy Law 375, 380.

[111] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 163.

[112] Van Alsenoy (n 40) paras 1238-1239.

[113] See in that respect *Google Spain* (n 32) para 34; *Wirtschaftsakademie* (n 31) paras 26, 28; *Jehovan* (n 31) para 35; *Fashion ID* (n 31) paras 65, 66.

operations of the cloud provider remain unknown to the data subject. In this context, the cloud provider is not supervised by the cloud customer, who lacks real control and power, nor by the data subject, who additionally lacks relevant information. Cloud providers are ultimately constrained only by their reputation. It should also be noted that if the cloud provider qualifies as processor, the only interlocutor of the data subject is the cloud customer. Indeed, addressing data subjects' requests is the responsibility of the controller alone, the processor having a mere obligation to assist the controller. This circumstance could be problematic if the household exception stated in Article 2(2)(c) of the GDPR applies to the cloud customer. Even though the cloud provider would need to abide by the GDPR (as processor), as it must only assist the controller and not directly address the data subjects' requests, data subjects may have no one to assert their rights against if the cloud customer (as controller) does not need to respect the GDPR due to the household exception.[114]

II. TOWARDS ANOTHER QUALIFICATION BY EU REGULATORS

Cloud providers as controllers

The four characteristics presented above demonstrate, in our view, that cloud providers are more than processors. Whereas processors typically only implement the instructions of the controllers by virtue of the degree of control controllers exercise over processors,[115] cloud providers are specific insofar as they, ultimately, have important control and autonomy regarding the security measures, the storage and deletion of personal data (including the retention localisation), the choice of subcontractors, as well as the persons who can have access to the data. In addition, contrary to what is required in a controller-processor relationship, cloud customers are often not able to effectively request changes concerning the relevant data processing activities.[116]

These critiques are not (yet) shared by the majority of lawyers and policy-makers. However, Bhowmik stated that:

> Cloud computing vendors build data centers at locations of their convenience, both

[114] Kamarinou, Millard and Turton (n 42) 298.

[115] European Data Protection Board, 'Guidelines 07/2020' (n 22) paras 80, 83.

[116] *ibid* para 30.

> geographical and economical. (…) Since subscribers remotely access cloud computing over the Internet, they may not be aware of the actual location of the resources they consume. (…) Most regulatory frameworks recognize cloud consumer organizations responsible for the security, integrity, and storage of data even when in reality it is held by an external cloud vendor.[117]

Bhowmik thus addresses – or even implicitly criticises – the existing duality between the factual control over the data on the one hand, which rests with the cloud provider, and the legal 'control' – or responsibility – on the other hand, which rests with the cloud customer.

Against the background of the four characteristics presented in the previous section, in the context of the storage of personal data, cloud providers present features that make them a better fit for the concept of joint controllers.

Regarding the qualification of cloud providers as controllers, like the example given by the EDPB of a service provider qualifying as controller (the Taxi service example[118]), cloud providers have designed their infrastructure and services without any instructions from cloud customers. Cloud providers also determine essential means of processing and therefore act as controllers, notwithstanding the fact that the processing activities occur further to a request of or consent by cloud customers.

As already discussed, cloud providers possess actual decision-making power over the following essential means: the security measures, the storage and deletion of personal data, the choice of subcontractors as well as the persons who can have access to the data.

The question whether cloud providers determine the purpose of the data processing activity is however not so clear-cut as the determination of the essential means. First, from a theoretical perspective, in the

[117] Bhowmik (n 4) 47. Bhowmik refers to the term 'cloud consumer organizations', whereas we deliberately use the concept of 'cloud customers' in this article. We prefer the latter, since 'consumers' generally imply natural persons, while cloud customers can be either natural or legal persons.

[118] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 82. The taxi service example given by the EDPB concerns an online platform allowing business customers to book a taxi. The EDPB clarifies that the provider of the online platform qualifies as data controller because it has designed its platform as part of developing its business activity, and without any instructions from its customers. It is also the taxi service provider, which determines the categories of personal data it collects, as well as the data retention periods. Thus, despite the fact that the personal data processing activity takes place following a request from its customers, the EDPB states that the provider of the taxi service platform still qualifies as controller. While cloud providers and the provider of such an online platform differ in many respects, the key criterion identified by the EDPB to qualify the provider of the platform as controller – the design of the service without any instruction from the customer – also applies to public clouds.

recent *Fashion ID* case[119], the CJEU confused the purpose requirement by asserting that a mere economic interest would satisfy the purpose requirement.[120] The EDPB however clarified that a mere commercial benefit does not suffice.[121] Second, in the present case, and as explained above, it is clear that the 'why' of the data processing activity, *i.e*. the specific reason thereof, lies with the cloud customer.

Despite the above uncertainties, if we step back from the purpose requirement considered alone, the EDPB admits that the essential means are closely linked to the purpose and scope of the processing.[122] The implication would be that the determination of the essential means would automatically entail the determination of the purpose. In any event, whether or not the cloud provider determines the purpose of the processing activity is not determining for the qualification as controller, as only the latter can determine the essential means.[123] We hence agree with other scholars, who believe that the GDPR should rather have prescribed that the controller must determine the purpose *or* the essential means of the relevant data processing activity.[124]

As cloud providers determine the essential means of the processing activity (as well as, arguably the purpose of the processing activity), they qualify as controllers, a qualification that was suggested already in 2011 by the renowned National Institute of Standards and Technology ('NIST') who allocated the tasks of security and privacy to the cloud provider.[125]

Cloud customers and cloud providers as joint controllers

Regarding the cloud customers, we do not object to the fact that they qualify as controllers. They certainly determine the purpose of the processing activity, as well as certain essential means, such as the

[119] *Fashion ID* (n 31).

[120] *Fashion ID* (n 31) para 80. See also Charlotte Ducuing and Jessica Schroers, 'The recent case law of the CJEU on (joint) controllership: have we lost the purpose of "purpose"?' (2020) 6 Computerrecht Tijdschrift voor Informatica, Telecommunicatie en Recht 424.

[121] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 68.

[122] *ibid* para 40.

[123] René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10(1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 39, para 18. As Mahieu puts it, even though the definition of controller requires a determination of both the purpose and means, 'Effectively, the question of determining the purposes *and* means is transformed into determining the purposes *or* the *essential* means'. See also European Data Protection Board, 'Guidelines 07/2020' (n 22) para 40.

[124] Mahieu, van Hoboken and Asghari (n 126), para 18; Van Alsenoy (n 40) para 1190.

[125] Liu and others (n 19) 3.

type of personal data that will be processed and the data subjects concerned as well as, to a certain extent, the duration of the processing and the recipients.

In this context, the cloud provider and the cloud customer do not make common decisions as to the purposes and the means, but make converging decisions, which influence the processing activity to different extents and at different stages.[126] They make decisions that are complementary and have a determining influence on the personal data processing activity. Concretely, it is because of the concrete decisions made by the cloud customer on the one hand (regarding the personal data, the data subjects, the duration and recipients) and the cloud provider on the other hand (regarding the security measures, the storage and deletion of personal data, the choice of subcontractors as well as the persons who can have access to the data) that the personal data processing activity occurs in this particular way.

It is worth noting that the Slovenian Data Protection Authority ('DPA') has recently qualified a cloud provider as joint controller. The Slovenian DPA followed some of the arguments we have put forward in this article, such as the lack of control of the deemed controller (the cloud customer) over the technical and organisational measures, the choice of the processors and the data retention periods. The Slovenian DPA also observed the lack of real instructions from the cloud customer to the cloud provider.[127]

Change coming from EU Regulators

In our view, the change of interpretation - or at least a case-by-case approach taking into account the role of cloud providers vis-à-vis the means of processing - should come from the EU regulators, the EDPB and the EDPS, respectively charged with the interpretation of the GDPR and the Regulation 2018/1725[128]. They would ensure a harmonised application of the GDPR throughout the EU. In light of the still increasing economic importance of the cloud, as well as the legal challenges it creates, the EU regulators should not wait for the CJEU to change the interpretation. EU regulators would not need to

[126] European Data Protection Board, 'Guidelines 07/2020' (n 22), paras 54, 63.

[127] Informacijski Pooblaščenec (0612-23/2019/19, 1 June 2022) < https://gdprhub.eu/images/8/89/IP_%28Slovenia%29_-_0612-23-2019-19.pdf> accessed 27 October 2022.

[128] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018], OJ L295/39. This Regulation applies specifically to the EU institutions and bodies, such as the European Commission, the European Central Bank, the European Parliament, etc. It also uses the criteria of the determination of the purposes and the means for the controller (Article 3(8) and, as regards the processor, of the processing of personal data on behalf of the controller (Article 3(12).

interpret the GDPR beyond its provisions; they would need to give the full effect to the already existing criterion whereby the determination of the essential means triggers the qualification as controller.

Allocation of responsibilities between the joint controllers

Even if cloud customers and cloud providers were qualified as joint controllers, they would not necessarily share equal responsibilities.[129] Responsibilities should be allocated to the entity which has the best ability to fulfil them.[130]

The EDPB proposes the following (non-exhaustive) list of responsibilities to allocate within the arrangement that joint controllers must enter into pursuant to Article 26 of the GDPR: implementation of general data protection principles, legal basis of the processing, security measures, notification of a personal data breach to the supervisory authority and to the data subject, data protection impact assessments, use of a processor, transfers of data to third countries, organisation of contact with data subjects and supervisory authorities.[131]

In our view, in the context of the storage of personal data, the cloud provider would be the main entity responsible for the integrity, confidentiality and security of the data. More specifically, the cloud provider should be the main responsible entity for the security of the systems it manages (*i.e*. at the very least, the security of the facility, servers, network and layer of virtualization). Conversely, the cloud customer would rather be responsible for the security of the components it manages. Overall, even though the security of the data subjects' data largely depends on the cloud provider[132], it is a shared responsibility between the cloud customer and the cloud provider.[133]

In the same vein, the cloud provider would be best suited to predominantly own the responsibility of the use of a processor, as well as the transfer of personal data to third countries.

The cloud customer would be better placed to take on the responsibility for the choice of a legal basis for the processing activity, the contacts with data subjects (including to perform the transparency

[129] *Wirtschaftsakademie* (n 31) para 43. This has been confirmed in *Jehovan* (n 31) para 66 and in *Fashion ID* (n 31) para 70. See also European Data Protection Board, 'Guidelines 07/2020' (n 22) para 169.

[130] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 168.

[131] *ibid* para 166.

[132] Bhowmik (n 4) 46.

[133] Liu and others (n 19) 16; Bhowmik (n 4) 104, 270, 299.

obligations and address the data subjects' requests, with the cooperation of the cloud provider) and supervisory authorities, as well as to respect the data minimisation and accuracy principles. The implementation of a data protection impact assessment should also be borne by cloud customers.

Regarding the other principles listed by the EDPB, it is more complicated to find a clear delineation of responsibilities. Thus, the principles of purpose and storage limitation would need to be assumed by both the cloud provider and the cloud customer. The accountability principle will also need to be respected by both entities for the obligations they respectively own.

Obviously, even though we have tried to set out some of the key guiding principles that ought to frame the allocation of responsibilities, it will ultimately depend on the individual characteristics of the instances of cloud computing (among others on the services offered by the cloud provider, and the service model – IaaS, PaaS, or SaaS). In other words, the allocation of responsibilities should be assessed on a case-by-case basis.

Normative interest of the joint controllership qualification

As already mentioned, we argue that the prevailing view leads to undesirable consequences, harming cloud customers and, in particular, data subjects. However, if adopted by the EDPB and EDPS, the joint controllership qualification would solve or at least mitigate the identified issues.

First, as controllers, cloud providers would be subject to more obligations than as processors, as the prime recipient of the data protection obligations remains the controller, while the processor is only subject to specific contractual and legal obligations. In addition, according to Article 82(2) of the GDPR, controllers are liable if they are 'involved in' a processing activity causing a damage to a person. The processor however is only liable to the extent that it has violated its contractual or legal obligations.[134]

Because of these two reasons (additional obligations and higher liability exposure), cloud providers would (need to) demonstrate a higher level of accountability in the sense of Article 5(2) of the GDPR, which would result in more transparency and control for data subjects. Of course, the joint controllership model would increase the compliance costs for cloud providers.

Second, the joint controller model we propose better fits the current definitions of controller and

[134] Van Alsenoy (n 40) paras 181, 184, 193, 195, 196, 200,

processor enshrined in the GDPR, as well as the factual reality. Therefore, the obligations would be better allocated to the entity that is able to respect them. In other words, there would be a better correlation between the liability framework and the ability to exert an influence over the respect of obligations.[135] This would be fairer in terms of the accountability and liability of cloud customers and cloud providers.

Furthermore, as per Article 26 of the GDPR, cloud customers and cloud providers would need to allocate among them the set of responsibilities enshrined in the GDPR. That allocation would be determined in reference to the entity best suited to fulfil certain obligations.[136] This arrangement should, as a result, avoid loopholes where some responsibilities are not at all attributed.

On the side of the data subjects, pursuant to Article 26(2) GDPR, they would at least receive information about the key aspects of the arrangement between the cloud provider and the cloud customer, thereby enabling them to identify the relations between the joint controllers in the context of the processing of their personal data. As a result, they would be better capable to exercise their rights against the controller of their choice (Article 26(3) of the GDPR) and control the respect of the GDPR.

Finally, the application of the household exception (Article 2(2)(c) of the GDPR) would not lead to a situation where data subjects would have no entity to assert their rights against. Indeed, if the cloud provider qualifies as a controller, data subjects exercising their rights would find an entity under the obligation to respond to their requests. Against that background, the qualification of the cloud provider as controller is not only more logical, but also more appropriate to safeguard the rights of cloud customers and, in particular, data subjects. On account of the enhanced protection of data subjects, the joint controllership interpretation is thus better aligned with the core objective of the GDPR.[137]

CONCLUSION

The current controller-processor model that is applied to the cloud mainly results from the initial choice made by the cloud customer to initiate a relationship with the cloud provider, as well as from the alleged

[135] Ivanova (n 110) 15; Wong (n 110) 380.

[136] European Data Protection Board, 'Guidelines 07/2020' (n 22) para 168. See also Van Alsenoy (n 40) paras 1238-1239.

[137] *Wirtschaftsakademie* (n 31) para 28. This has been confirmed in *Jehovan* (n 31) para 35 and in *Fashion ID* (n 31) para 65.

consent that the cloud customer gives to the cloud provider. The actual degree of control of the cloud customer lacks a thorough analysis. Such analysis however indicates that cloud providers have a significant degree of control over the personal data and some essential means. We argue that this control results from four factors, *i.e.* the control of the underlying architecture by the cloud provider, the very purpose of the cloud, the power asymmetry that largely weighs in favour of cloud providers and finally, a new legal framework that tends to assign more responsibilities to cloud providers.

Because the joint controllership model better matches the current technological and economic reality, we believe that EU regulators should give it more consideration in the context of the storage of personal data. This model has already found some resonance within a decision rendered by the Slovenian DPA and it is also the approach that computer scientists and engineers would follow. Finally, the joint controllership interpretation would provide a fairer responsibility and liability framework for cloud customers and providers, and most importantly - bearing in mind the purpose of the GDPR - an enhanced protection of the data subjects.