derecom

ISSN: 1988-2629. Nº. 27. Nueva Época. Septiembre 2019-Marzo 2020

Cómo citar este texto:
Kwiatkowska, M. (2018). Negotiating a data processing agreement: a practical perspective. *Derecom*, 27, 181- 190, http://www.derecom.com/derecom/

NEGOTIATING A DATA PROCESSING AGREEMENT: A PRACTICAL PERSPECTIVE

LA NEGOCIACIÓN DE UN CONTRATO DE PROCESAMIENTO DE DATOS PERSONALES: UNA PERSPECTIVA PRÁCTICA

© Monika Kwiatkowska
Ping Identity Corporation (Reino Unido)
m.zwolinska@yahoo.com

Summary

Putting in place a data processing agreement between a data controller and a data processor (or a data processor and a data sub-processor) is a requirement for data processed within the scope of GDPR. This document, which is a proper contract between the two parties, aims to ensure that everyone involved is handling personal data in accordance with GDPR's stipulations and in line with the rules pre-established by the parties. Most importantly, it lays down requirements for data processors to meet before they are trusted with the data provided by the data controller. Both data controller and processor are, however, often driven by divergent interests when establishing such document. Main challenges are the ones relating to: responsibility for determining the scope and types of data processed; obligations to assist and cooperate; liability for implementation of adequate security measures and for security incidents; exercising data subjects' rights; questions relating to data residency and international data transfers; use of sub-processors; timeframe for notification obligations, etc.

The paper is a practical perspective on how these different issues are addressed by the business and what arguments can be raised by each party when discussing various aspects of the data processing.

Resumen

Establecer un acuerdo de procesamiento de datos entre un responsable del tratamiento de datos y un encargado del tratamiento de datos (o un encargado del tratamiento de datos y un subencargado del tratamiento de datos) es un requisito para los datos procesados dentro del ámbito del RGPD. Este documento, que es un contrato adecuado entre las dos partes, tiene como objetivo garantizar que todos los involucrados estén tratando datos personales de acuerdo con las disposiciones del RGPD y de acuerdo con las normas establecidas por las partes.

Recibido: 14/03/2019 Revisado: 30/07/2019
Aceptado: 16/08/2019 Publicado:15/09/2019

Lo que es más importante, establece requisitos para que los encargados del tratamiento de datos los cumplan antes de que se confíen en ellos los datos proporcionados por el responsible del tratamiento de datos. Sin embargo, tanto el responsable del tratamiento de datos como el encargado del tratamiento a menudo están impulsados por intereses divergentes al establecer dicho documento. Los principales retos son los relacionados con: la responsabilidad de determinar el alcance y los tipos de datos tratados; las obligaciones de asistencia y cooperación; la responsabilidad por la aplicación de medidas de seguridad adecuadas y por incidentes de seguridad; el ejercicio de los derechos por parte de los titulares de los datos; las cuestiones relativas a la ubicación de datos y las transferencias internacionales de datos; el uso de subencargados: el plazo para las obligaciones de notificación, etc.

El artículo ofrece una perspectiva práctica sobre cómo estas diferentes cuestiones son abordadas por la empresa y qué argumentos puede plantear cada parte al debatir varios aspectos del procesamiento de datos.

Keywords: Data Processing Addendum. Processing of Personal Data. Data controller. Data processor. Data sub-processor.

Palabras clave: Addenda sobre el tratamiento de datos. Tratamiento de datos personales. Responsable del tratamiento de datos. Encargado del tratamiento. Subencargado del tratamiento de datos personales.

1. Introducción

Data processing agreements, otherwise referred to as “controller-processor agreements”, “controller-controller agreements”, or “joint-controller agreements” are required under Article 28 of the General Data Protection Regulation (GDPR). This regulation applies within the territory of European Union and to activities of entities doing their business in European Union. Article 28(1) imposes that a controller only uses processors that provide sufficient guarantees that data processing will meet the requirements of the GDPR.[1] These agreements lay out the ground rules for any handling of personal data done by a processor on behalf of a controller. They ensure any such data processing is in accordance with the requirements of GDPR and any other applicable laws. There is, however, a number of challenges the parties face when negotiating a Data processing agreement. To begin with, whether such agreement is required or not can be a point of contention. A party may argue that although they do process data, none of this data is personal data in the meaning of data protection laws. Similarly, it may be argued that none agreement is needed as no EU data subjects’ data are processed. How can one really identify and distinguish data subjects’ provenance in a digital world, where not only identification would need to be based on person’s nationality, but also their geographical location? Furthermore, a software provider may argue that because the product they supply is delivered to the other party, installed on their premises and managed by them without the software provider’s intervention – no data is processed by such supplier and therefore no agreement is required. The existence of the need for such contract is an argument itself, as negotiations may be somehow cumbersome. From a high level perspective, most conflicts result from, on one hand, different interpretations of the regulation and the way this should apply to the specific data processing or the specific party and, on the other hand, from each party’s operational practices and capacity to adjust those to other party’s needs. A number of areas can be identified as the ones where confrontation occurs most often. Six of those areas are contemplated below. They have been identified as either the most recurrent (international data transfers; audit; notification timeframes), fundamental (in a sense that as such, they determine what direction the whole negotiation process will take: definition of parties' roles) or contentious (sharing data with data sub-processors; liability).

I. **Determining each party's role** - One of the first steps in constructing a Data processing agreement is determining whether the organization is functioning as a controller or a processor. In accordance with Article 28 of GDPR, a controller is the natural or legal person who "determines the purposes and means of the processing of personal data," whereas a processor is the person who processes personal data on the controller's behalf. The distinction is essential because depending on how the roles will be assigned, the party's exposure and accountability will vary significantly[2]. In fact, the European Commission's guidance holds the data controller to be the principal party responsible for collecting, managing, and providing access to data[3]. Data controllers are the ones collecting personal data from data subjects. With that regard, they are responsible for determining their legal authority to obtain that personal data, as well as establishing a legal basis for such collection using one of the six available lawful bases featured in the GDPR. It can be a fine line, however, between controller and processor because as soon as the processor becomes involved in collecting data, they become a data controller either separately or jointly with the party initially acting as the sole controller[4]. Whether the given use case will have to be classified as a data processor – data controller relationship, or a relationship between two independent data controllers, or even joint controllership – depends on a number of factors and the answer is rarely an obvious one. One needs to look into whoever is the dominant actor in determining the purpose and means of the processing, whether anyone has the freedom to start additional processing, to what extent the party is involved in deciding which data attributes are to be collected, whether these are anonymized or not, etc. Moreover, although the creation of the data processing agreement is the responsibility of the data controller and the data processors are obligated by law to follow the instructions provided by the controller - if the controller fails to outline the required processes as part of the agreement and leaves the methods and means up to the processor, then the processor may morph into the controller in the eyes of the law. Within that context, the way the parties will negotiate their role will largely depend on the level of liability they wish to expose themselves to. In most cases, the parties' preference is to keep as much control as possible over what data is collected, how it is obtained and on what legal basis. The controller is also responsible for what data exactly will be shared with data processor for processing, although it is in processor's interest to require some contractual safeguards to protect themselves from being sent any other types of data than the ones agreed upon in the contract. Being a data controller also means one remains the effective owner of the data and can therefore determine what it can be used for and what other information can be drawn out of it which is particularly important in the era of Big Data[5]. It is not uncommon however, that a party will aim in limiting its responsibility to the strict minimum, in which case they will argue that their intervention is solely restricted to fulfilling controller's instructions as to how to process the data provided to them[6]. Also, as part of the parties' relationship, they might act as controller or processors interchangeably depending on the type of data and the processing operation. Eventually, it might make more sense to identify each party's realistic obligations clause by clause rather than classifying them as processor and controller throughout the whole agreement.

II. **International Data transfers** – One of the most essential requirements for the data controllers is the one to make sure that data transfers to jurisdictions other than the ones where these have originally been collected are always carried out in compliance with applicable regulations. Thus, on international level, data can only be transferred to countries for which European Commission has confirmed that they ensure adequate level of protection of personal data or, alternatively, another legal mechanism has been put in place to ensure that security[7]. To that point, parties will often need to negotiate as part of a Data processing agreement which type of legal basis they consider sufficient for international data transfers. American-based companies, who very often rely on their Privacy Shield Certification for transfers between European Union and/or Switzerland and United States, face this argument when they endeavor to convince their business partners that this certification is a reliable mechanism for data transfers and one that provides for as much safety as the Standard Contractual Clauses do[8]. One should not forget that, despite the controversy underpinning the Privacy Schield scheme, the validity of Standard Contractual Clauses has also been protested on several occasions – which renders those two instruments similarly attractive to the business. In both cases, it is safe to say that some provisions should be included in the agreement to address the risk of either the Privacy Shield scheme or Standard Contractual Clauses being revoked – in which event the parties should agree in advance whether the processing should automatically be stopped and the underlying commercial agreement automatically terminated; or whether the processor provides a warranty that they will implement an alternative mechanism to ensure all data transfers remain lawful; or simply that parties will cooperate in good faith on agreeing a mutually acceptable solution. Determining contract termination as one of the available remedies can also raise discussion as the processor might argue that their inability to transfer data abroad results from a regulatory change which they had no control over and as a consequence, controller's right to terminate would appear as a disproportionate way to penalize the processor.

III. **Sharing data with data sub-processors** – It is in data controller's interest to require from the data processor to not disclose any of the data to sub-contractors for further processing, unless these are first approved by the data controller. This allows control over the dataflow and is consistent with controller's need to ensure compliance with data protection laws throughout the whole chain of the data processing. It often goes against the data processor's need, as the data processor may typically be using several sub-processors for processing of data, whether this would be for maintenance of a data center, provision of a data management tool or certain cryptography services. Disclosure of data will, therefore, in many cases, be a non-negotiable requirement from the data processor. In addition, wherever the data processor would be processing data on behalf of multiple data controllers, it might not be able to subject the use of its data sub-processors to the consent of one particular data controller. Handling such individual consents would be highly impractical and risks to place data processor in a position where one data controller could prevent all other controllers from a desired functionality because of inability to use the given sub-processor. Hence, as part of negotiating a Data processing agreement, data controller and processor can put in place a system of notification of the desire for the data processor to utilize services of a new data sub-processor, which in conjunction with a data controller's right to object to such use would constitute a more flexible method of scrutiny for sub-processors in question. In such a system, instead of requiring a prior, written consent to use a data sub-processor, data processor would be free to use the sub-processor as soon as they have informed the data controller of such use and have given them time to object. To complete the whole process, it is advisable that parties agree that any such objection should be based on objective criteria and have reasonable ground. Often a Data processing agreement would include a list of grounds based on which data controller can raise its objections: non-compliance with applicable law or regulation, undesirable location of the data sub-processor, incompatibility with other third parties involved with the data processing on behalf of the controller, etc. Language around the acceptance of a new sub-processor being deemed as soon as the objection has not been raised within a specified period of time can certainly be helpful - so can establishing what the consequences of any such objection should be. To definitely avoid the situation where one data controller could block the use of a sub-processor for other of data processor's customers, it is essential to give the data processor few options for how such objection should be handled. For instance, data processor should be provided with time and room for suggesting a use of an alternative data sub-processor, whether this would then be applied to the entire data processor's customer base or the objecting data controller specifically. Other option can be for the data processor to be able to take corrective actions to address any of data controller's concerns around appointing the new sub-processor – but the parties need to make sure to define a specific timeframe to avoid unnecessary delays. Eventually, a right to terminate the engagement should be made available to data controller who cannot accommodate using the new sub-processor and in such case, in case any fees for the product or service have already been prepaid, these should be refunded pro-rata. It is also essential from the data controller perspective that the data processor remains liable for any of its sub-processors acts and omissions: data controller has no visibility over nor direct relationship with the data sub-processors so this in case of any violation by the sub-processor, claims should be handled directly between the data controller and the data processor in accordance with the negotiated terms.

Furthermore, any disclosure of data to a sub-processor must be made based on a valid agreement that will ensure continuity in providing appropriate safeguards. Data processors will often take a position that the Onward Transfer Agreements they execute with their sub-processors will include processing obligations in line with applicable privacy laws and the Data processing agreement under negotiation, but that they cannot commit to incorporating exactly the same provisions as included in the Data processing agreement. This is most of the time related to the fact that many of the sub-processors in question are the market leaders in their field, with whom the data processor will not have leverage to raise other than standard requirements, or any requirements really that go beyond these sub-processors' general terms and conditions. This would be, for instance, true for service providers who utilize data centers to host data they process or who use a customer relationship management software to administer personal data of their customers. Although they may strive for flowing-down any measures the data controller requires from them to put in place onto their sub-processors, they might, in reality, simply not be able to impose exactly same obligations. In the end of the day, what counts is that the obligations they manage to incorporate in their agreements are materially consistent with the ones agreed between data controller and data processor. This, in addition to data processor's liability for its sub-processors, should give the data controller sufficient comfort around appropriate technical and organizational measures being adopted throughout the whole chain of dataflow. For most efficient control, data processor should also contractually commit to carry out annual reviews and assessments of its sub-processors to ensure they maintain proper safeguards to protect data they process.

IV. Notification timeframes – GDPR provides for several types of obligations for the data processor to notify the data controller of various events in connection with the personal data being processed. Although most of the time, the data controller is the one directly exposed to the regulators or data subjects (based on the fact that data controller's use of the data processor is not always of public knowledge), there might be scenarios where the regulator or the data subject reaches out to the data processor directly to exercise their rights over the data being processed. Data controller is, however, the one responsible for addressing any such requests and therefore it needs to make sure some contractual safeguards are put in place to govern cooperation with data processors with that respect. First of all, the data processor should be required to notify the data controller of any request for access to data from any regulatory body or government official, as well as of any warrant, subpoena, or other request regarding the data. Secondly, the obligation of notification should also arise with respect to any requests and complaints of data subjects. To the extent legally permitted, data processor should be under obligation to inform data controller that it has received any such request and this should be achieved within a specified period of time. This should refer to such requests as opt-outs, requests for access and/or rectification, erasure, restriction, data portability, but also any type of data subject's complaint, notice and can even be defined as englobing any kind of communication by the data subject to the data processor in relation to how their personal data is collected, accessed, used, stored, processed, disposed of and disclosed. For more clarity, it might also be beneficial to expressly state in the Data protection agreement that the data processor should not be responding to any of this type of requests unless specifically authorized and directed to do so by the data controller or required under applicable law. Parties may also consider to add some language around reasonable cooperation with respect to responding to any such request. Some data processors will reserve a right to charge a fee in assisting the data controller in responding to these requests. Although this right is not expressly set forth in GDPR, the argument is based on the fact that in accordance with article 15(3) thereof, the controller is entitled to charge a fee for data subject's requests in excess of 1. This right is aimed to cover any potential administrative costs which is why it might make sense that, since the data processor, is also suffering such cost when assisting the data controller, it should be able to recover its part. From data processor's perspective, this helps alleviating undue administrative burden caused by the fact that the data controller has shifted the responsibility for handling the data subjects' requests to the data processor. The data controller's aim should be, within that context, to only agree to pay reasonable fee to the extent it was able to recover same fee from the data subject.

Furthermore, one of the core elements of a Data processing agreement is the language governing security incidents notifications. Article 33 of GDPR imposes a duty on data controllers to report certain types of personal data breach to the relevant supervisory authority. This must be accomplished within 72 hours of becoming aware of the breach, where feasible. Moreover, in the event the breach is likely to result in a high risk of adversely affecting data subjects' rights and freedoms, data controller must also inform those individuals without undue delay. The difficulty is that most data controllers interpret this 72h timeframe as a delay that starts at the time of the incident. As a result, they flow down an obligation to notify to their data processors which is significantly less and usually sits somewhere between 12 and 48 hours – which therefore allows the data controller to still keep the margin once they receive notification and before they pass it on to the regulator. Such requirement may lead to a conflict of interest between the data controller and the data processor, in a sense that reporting a security breach within a 72h period (which does not take into account the business reality of weekends, bank holidays, time difference, etc.) is already a significant undertaking for any organization and involves the development and provisioning of a comprehensive containment plan – let alone if this becomes a 12 or even 48h condition. In reality, however, data controllers omit to understand that this timeframe only applies once they become aware of the incident which means that whatever time the data processor has spent in discovering, analyzing and reporting a breach does not count towards the 72h deadline. What GDPR requires from data processors in its article 33(2) is to provide notification to data controllers "without undue delay". It still makes sense to put some kind of timeframe for such notification, since otherwise data controllers might not feel they can be held accountable for rendering their processes as efficient as possible. There is no point, however, in requiring that this sits well above 72h, especially when the agreement is negotiated with a data processor who relies on the data centers where data is processed in a multi-tenant, single instance environment. Once such data processor becomes aware of a data breach, there is a significant number of checks and processes it will need to implement to ensure the source of the breach has been properly identified and only the relevant data controller is informed of the incident. It is, however, advisable, that the data controller requires that data processor takes any steps as the parties deem necessary and reasonable in order to remediate the cause of the incident (to the extent, of course, that the remediation lies within the data processor's reasonable control. From the data processor perspective, and particularly - but not only - in the context of the afore-mentioned multi-tenant environment, data processor should seek to limit its obligations of notification or remediation by carving out scenarios where the data controller in question would be the one, directly or indirectly, causing the breach or, alternatively, by requesting that in such case any costs suffered as a result of the steps undertaken by the data processor were reimbursed by the data controller at fault[9].

V. Audit - Another controversial subject in scope of a Data processing agreement is data controller's right to audit data processor's processes, as well as the processes of any data sub-processors involved. Most software and Saas [software as a service] providers have a default position of not allowing any on-premise audits of their production and non-production environment, whether that was to be carried out in their own systems or within the infrastructures of their sub-processors. With respect to this last scenario, and similarly to the issue of any security measures being flown down from the agreement between data controller and data processor to the one between data processor and data sub-processor, the data processor might simply not be in a position to negotiate any audit rights with its sub-processors other than the ones they offer as part of their general terms and conditions. The reality will very often be that audits should be limited to the data processor sharing the results of its third party audits with the data controller for review and optionally providing answers to security questionnaires the data controller may put in front of it. The third party audits would usually be in form of industry certificates, results of intrusion testing and statements of compliance with applicable standards and will detail data processor's organizational and technical measures implemented to process data in secure manner. An issue may arise whenever the data controller is actually required to ensure an on-site audit of itself and any data processors it uses based on a regulation – whether this results from a national implementation of GDPR or because of the data controller's regulated industry it operates in. In any case, any type of audit the parties agree for the data controller to be granted with should only be carried out in accordance with a set or pre-established rules around the scope, planning and duration. Usually, it comes without saying that the cost of an audit should by default be borne by the data controller unless such audit reveals a number of inconsistencies on the data processor's side or that the data processor has engaged in any fraudulent activities.

VI. Liability – The allocation of risk — and thus the issue of the liability cap — plays an important role in the negotiations of Data processing agreements. It needs to be carefully considered by both the data controller and data processor as exposure to data subjects' claims or regulatory fines constitutes a substantial financial risk[10]. One of the changes introduced by GDPR has been the shift of responsibility towards both data controllers and data processors rather than data controllers only (who, under the previous law, would have to then act against the data processor at fault to recover losses). Although GDPR does not specifically address the limitations of liability to be put in place between the parties, nor does most of the guideline documentation[11], several provisions outline general principles to be followed with that respect. On the one hand, article 82 of GDPR forbids exclusion of liability towards the data subjects and the supervisory authority imposing a penalty. On the other hand, it states that either party may exclude their liability if "*it is not in any way responsible for the event giving rise to the damage*". Subject to these rules, the parties are free to establish the applicable liability system as they wish: whether they would opt for a full liability of the party who commits the breach or a joint liability allocated proportionally to their fault. It is also advisable that a mechanism of conciliation or ad hoc mediation is agreed upon.

Data controllers will very often require that data processor accept uncapped liability for the obligations they agree under the Data processing agreement. This is a highly sensitive topic which needs to also involve a thorough analysis of the volume and nature of the data being processed. Data processors will typically insist on a cap on their liability – which they might want to have aligned on whatever limitations have been agreed in the master agreement or which can also be set up as a super cap specifically crafted for the processing of personal data. One of the options to consider (and current trend) is for the cap to be proportionate to the data processor's cybersecurity insurance coverage, although the amounts data processors are insured against are often aggregate ones and therefore do not represent an adequate threshold. Furthermore, the events that are likely to trigger party's liability also need to be carefully considered. For instance, if appointing a new data sub-processor requires from data processor to obtain a prior consent from the data controller, then failure to do so will expose it to a claim, whereas the risk would be more manageable if such appointment was only subject to a notification with a right to object or, even more so, if the data controller would have given its general consent by default[12].

Frustration arises as each party needs to compromise and the end result of the negotiation is usually that the cap, as agreed, represents an unreasonable financial exposure from the data processor's perspective but insufficient financial safeguard from the data controller's perspective. To data processor's defense, unlimited liability, or an excessive cap, may not be justified on the grounds that in case of breach, the data processor will also have direct liability in front of the Supervisory Authority so the Data Protection Authority would most probably pursue the data processor directly rather than going first after the data controller. However, to data controller's point, despite the overall responsibility being shifted to both parties under GDPR, data controller can still be held liable for data processor's failings as it is ultimately accountable for the data processing in accordance with section 5(2). At the end of the day, under section 82(3), it's only when one party has definitely not contributed to the existence of the data breach that it can avoid being jointly held responsible with the other. Ensuring appropriate safeguards in the Data Processing Agreement seems to be the most straight forward way, on the one hand, to avoid accusations around data controller's failure to exercise sufficient due diligence over the data processor and monitoring its compliance in appropriate manner and, on the other hand, to pro-actively address such issues as data controller's unlawful instructions or inaccuracy of data provided.

A number of steps can be followed to facilitate conclusion of a Data Processing Agreement. Definition of each party's role – whether an independent controller, joint controller or processor – is fundamental as it will determine how all other decisions are going to be made, who will follow whose instructions, who will need to implement security measures, who will remain accountable for the data etc. An extensive data mapping helps visualizing the data processes contemplated by the parties and is usually an efficient tool in defining who does what. Transferring data on international level presents a challenge in the light of most of the legal instruments supporting such transfers being currently challenged in the courts. Nonetheless, these remain valid until further notice and the best way to ensure that appropriate legal safeguards are implemented is to follow all guidance and recommendations from data protection authorities. Data shared with sub-processors is still data the processor remains fully accountable for and it cannot be stressed enough how important it is for the processor to ensure appropriate contractual arrangements are in place in support of the Data Processing Agreement. These include both provisions regarding how data controller's consent shall be collected for use of sub-processors, as well as contracts with these sub-processors which need to reflect substantially same restrictions and obligations with respect to data as those contained in the Data Processing Agreement. Notification timeframes to be agreed between the parties have to, first of all, be within the limits prescribed by the regulation to allow both data controller and processor to remain in compliance. But secondly, they also need to be aligned with what the data processor can realistically implement from the perspective of its internal processes, operations and resources. A variety of productivity and management tools have recently been released on the market to help companies improve their internal efficiency, potentially enabling data processors to offer fast response in case of a data incident or a data subject access request. With regard to audits, these continue to be a source of tension but the diversity of hosting solutions available on the market (private tenancy, multi-tenancy, internal cloud) gives hope that practices will follow to adapt to these different environments in a way acceptable for both controllers and processors. Finally, liability for data processing is at the heart of the negotiation of the Data Processing Agreement and will surely always be the area where most discussions take place. A reasonable approach, and a one where parties' mindset is not limited to straightforward indemnification system, is certainly a way to work out a balanced relationship where everyone will feel comfortable that they can stand up to their engagements.

As an overall recommendation, it seems that a starting point to negotiating a Data Processing Agreement should be the use of reasonable drafting which will address both data processor's and data controller's concerns and also take into account the financial and reputational risk they are facing. It is worth keeping in mind that, as far as the financial aspects go, depending on each party's global turnover, the fines it might face may vary and a balance between the parties should be sought when agreeing to specific clauses. Finally, in an effort to render the Data Processing Agreement as complete and clear as possible, the parties should try not to become excessively prescriptive so that once agreed upon, the agreement can survive potential changes in the legislation without having to be amended except in the event its contents require material adaptation.

[1] CLARKE, J.. (2018). *Data-processing agreements from 30,000 Feet*, May 22, https://iapp.org/news/a/data-processing-agreements-from-30000-feet/. (accessed 16th Nov. the 16th, 2019).

[2] ICO. (no year). *Data controllers and data processors: what the difference is and what the governance implications are*, (versión 1.0), https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf. (accessed 16th Nov. the 16th, 2019).

[3] EUROPEAN DATA PROTECTION SUPERVISOR. (2018). "Guidelines on the protection of personal data in IT governance and IT management of EU institution", 23 March.

[4] KELLER, M.. (2017). *Data processor´s responsabilities under the General Data Protection Regulation*, LLM Thesis, Helsinki: University of Helsinki.

[5] HULL, G..(2015). “Succesfful failure. What Foucault can teach us about privacy self-management in a world of Facebook and Big Data”, 17 (2), *Ethics and Information Technology.*

[6] WEBBER, M. . (2016). “The GDPR´s impacto n the cloud service provider as a processor”, *Privacy Data Protect Law*, 16 (4): 11-14.

[7] SCHWARTZ, P.M.. (2019). “Global data privacy: the EU way”, February, 20, *New York University Law Review*, vol. 94.

[8] EUROPEAN COMMISSION. (no year). “Data transfers outside the EU”, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en.

(accessed 16th Nov. the 16th, 2019).

[9] MILLARD C.W. (Hon.), WALDEN I.. (2012). “Who is responsible for *personal data* in cloud computing?—The cloud of unknowing”, Part 2. *Int Data Privacy Law* 2(1):3–18.

[10] GRAY, J.. (2017). “GDPR Contracts and Liabilities Between Controllers and Processors”, September 8, https://www.insideprivacy.com/international/united-kingdom/gdpr-contracts-and-liabilities-between-controllers-and-processors/. (accessed 16th Nov. the 16th, 2019).

[11] “CNIL´S Guide for Processors in French and in English”, September, 2017.

[12] LEE, P. .(2017). *Managing unlimited demands for unlimited liability in GDPR contracts*, March 7, https://privacylawblog.fieldfisher.com/2017/managing-unlimited-demands-for-unlimited-liability-in-gdpr-contracts. (accessed 16th Nov. the 16th, 2019).