A processor in control
- A study of whether processors face increased liability under the General Data Protection Regulation

Michael Erici

Thesis in IT-Law, 30 HE credits
Examiner: Forename and surname
Stockholm, Spring term 2017
Table of contents

Abstract ........................................................................................................................................... 5
Introduction ........................................................................................................................................ 6
  Background ..................................................................................................................................... 6
  Research problems ......................................................................................................................... 6
  Method and sources ....................................................................................................................... 6
  Delimitations .................................................................................................................................. 8
  Disposition ...................................................................................................................................... 8
Objectives and intentions of the regulation ....................................................................................... 10
  Subject matter and objectives ......................................................................................................... 10
  Synopsis ......................................................................................................................................... 11
Defining a processor .......................................................................................................................... 12
  Processing of personal data ............................................................................................................ 12
  Case law regarding processing and personal data .......................................................................... 12
  The controller ................................................................................................................................ 14
  Case law about the definition of the controller ............................................................................ 15
  Synopsis ......................................................................................................................................... 16
Responsibilities of a processor under the directive .......................................................................... 17
  Regulated demands on the assignment of a processor ................................................................. 17
  Liability .......................................................................................................................................... 18
  Responsibilities of a controller under the directive ...................................................................... 18
  Standard, ASP 06 ............................................................................................................................ 19
  Synopsis ......................................................................................................................................... 20
Responsibilities of a processor under the new regulation ................................................................. 21
  Security .......................................................................................................................................... 21
  Documentation ................................................................................................................................. 21
  Cooperation with the supervisory authority and reports ............................................................... 22
  Assignment of a data protection officer ......................................................................................... 23
  Regulated demands on the assignment of a processor ................................................................. 23
  Liability .......................................................................................................................................... 24
  The responsibilities of a controller under the new regulation ..................................................... 25
  Synopsis ......................................................................................................................................... 26
An example, cloud computing ........................................................................................................... 28
  Definition of cloud computing ....................................................................................................... 28
  An example, storage using cloud computing ................................................................................ 28
  Synopsis ......................................................................................................................................... 29
Abstract

The new General Data Protection Regulation ("GDPR") will change the responsibilities for the actors that process personal data of EU citizens. In the directive, there is a clear distinction between a controller and a processor. The new regulation defines the different actors in a similar way as the directive while the responsibilities for the different actors’ have changed.

In the directive, the controller is solely liable for infringements. The processors responsibilities correlate to the contractual relationship with the controller. Under the new regulation processors will be directly liable for damages and fines. This will change the roles of the actors while definitions remain largely the same.

This thesis will study the changes going from the directive to the new regulation with regards to the definition of the actors, relevant responsibilities and liability. When the liability for the processor has been put in perspective the thesis will move on to look at the possibilities to limit or avoid liability through either contractual or technical solutions.

When the regulations have been studied, the thesis will analyse the definitions in relation to the actors responsibilities, the possibility to limit liability in relation to said responsibilities and if the level of liability can be seen as reasonable.
Introduction

Background

25th May 2018 a new regulation for protection of personal data will enter in to force. Legislation concerning the protection of personal data is nothing new. EU has historically covered the protection of personal data through directives; this regulation will take the place of these directives and be directly applicable in the member states.

The definition of the controller and the processor remains largely the same going from the directive to the regulation. The controller determines the means and purposes for processing personal data. The processor processes personal data on behalf of the controller. In the directive, the controller was held liable for not complying with the legislation. In the new regulation, the processor will be held directly liable for infringements to the regulation.

Research problems

To what extent can a processor be held liable according to the new regulation?

Could there be a need to rework the definitions of a controller and a processor following the changes in the responsibilities of the processor?

Is there a way for the processor to disclaim from their liability using contracts or technical solutions?

Depending on the conclusion of the above, is it reasonable for the processor to be held liable to the extent it is?

Method and sources

To reach a relevant conclusion regarding this subject one needs to study what is established law as well as what the law will be.

The legal dogmatic method is commonly referenced when it comes to legal research and sometimes not referenced at all since some authors consider it to be the judicial norm. The method can be described as a reconstruction of the judicial system. The legal dogmatic method

---

1 JP 2014 s. 216.
2 SvJT 2004 s. 5.
can be regarded as a positivistic method it aims to draw scientific conclusion based on a systematization of the judicial system.\textsuperscript{3} When it comes to analyzing the current directive, this method will be used and the directive itself will be studied together with case-law and other relevant sources to determine how the law currently shall be interpreted.

To analyze the regulation that is to be one must use a different approach. The law in its literal form is there for analyzing however there is a lack of established sources such as case law to give the paragraphs meaning. EU regulations lack the level of preparatory work that many national legislations produce. A more literal approach must be used while some clarity can be found by studying preceding rules and put them in relation to the new rules. This part of the research will also be based on the legal dogmatic method with the changes in method described above.

The technical development has a close connection to IT-law. To understand and apply the law one needs to understand the technical solutions used, as well as the possibilities for other technical solutions and put this in relation to the law. An understanding of the technology as well as the law is necessary to understand the limitations and solutions to legal problems.\textsuperscript{4} While not a classical source of law, the technical aspects of data and processing will be studied. With understanding of the technical possibilities and limitations not only can conclusions about what is required by the regulation directly through the demands on technical solutions be achieved, but also ways to comply with other requirements set out by the GDPR.

There have been disparities regarding how IT-law should be regarded. Some believe that the questions, arising from development and usage of IT can be solved using classic methodology and classical sources. Others believe that in order to achieve a better application one needs to understand the individuality of the questions arising in the digitalized society and connect them.\textsuperscript{5} In this thesis the latter view will be applied. The work will depend on the understanding of technical solutions in combination with the law to reach a conclusion.

To study contractual aspects in relation to the regulation, contractual principles on the international level will need to be considered. These can be found through soft law in the EU as well as globally.

\textsuperscript{3} SvJT 2004 s. 112.
\textsuperscript{4} Magnusson Sjöberg s. 25.
\textsuperscript{5} Siepel s. 162 ff.
Finally, the new regulation will be analyzed from a legally analyzing perspective to determine whether it will serve its intended purposes. The rules as they will be implemented will be put in relation to its purposes and the affects it could have on the possibilities for processing data and the market, therefore applying an external method.\(^6\)

**Delimitations**

This work will focus on the processor and the liability that follows with the new regulation. The responsibilities of the controller need to be studied to a certain extent since the definition of the processor as well as its responsibilities are tied to the controller. Rules applying to the controller will, however, only be studied to the extent that they grant an understanding of the processors liability. The rights of the data subjects will only be studied when needed to understand the objectives and purposes of the regulation.

Since the processor is the focus of this work the parts of the regulation that only concerns the relation between the data subject and the controller will not be studied.

National legislation will not be studied as a major part of this work; the purpose of the work is to understand relevant aspects of the regulation on a European level. Since it is a regulation it will be directly applicant to the member states therefore preceding national law will not be put in relation to the new regulation. However, national law can be used to show examples on implementation of certain articles from the directive.

Case law will be studied in areas where the regulation remains largely unchanged from the directive since said case law should be relevant for the new regulation as well.

**Disposition**

First the intentions and purposes of the regulation and the definitions of a processor and controller will be studied together with relevant case-law.

In the next chapters the rules in the directive and the new regulation will be covered. A concrete example will be given in the form of a cloud provider and how the changes in the regulation will affect it. The section will be tied together by a chapter where the differences of the directive and the regulation are highlighted while trying to find a conclusion to the roles and definitions

---

\(^6\) SvJT 2004 s. 134 ff.
of the actors. This chapter will take a legally analyzing approach in whether the roles and responsibilities are reasonable.

The next part of this work will look at possible solutions for processors to limit or exempt from liability through either contractual or technical means, both studied in separate chapters. The last chapter will try to answer the questions problematized in the thesis by analyzing the earlier work. This chapter will take a legally analyzing approach.

The different chapters will contain a brief introduction and summarizing synopsis tying them together. Sources will be given in a separate section at the end of this work.
Objectives and intentions of the regulation

There are no decisions by the court of justice yet on how to apply the GDPR. To reach a conclusion about how the new rules should be interpreted the objectives and purposes of the regulation need to be studied and applied to the articles.

This first chapter will study the objectives set out in the regulation. The objectives of the directive will only be studied to give the objectives context.

Subject matter and objectives

In its introductory article the GDPR sets out the material scope and objectives of the regulation. The Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” This article makes it clear that the purpose of the regulation is to protect the rights of natural persons and in the case of data protection that translates to the data subject.

The second objective of the GDPR correlates to the aspects of the free movement in the EU. “The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.” Naturally, high requirements on the actors will affect the market. Even though this objective addresses the free movement of data directly all increased regulation regarding a procedure should affect the market indirectly. To make it harder for processors to conduct business would result in more data stored locally which in turn means less trade with and movement of data.

The objectives of the GDPR are almost identical to the objectives of the directive. Relevant case-law directly applicable to the directive should largely be applicable to the new regulation as well since the objectives remain the same and the court will base their decisions on said objectives.

The European commission states on their webpage that. “The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single..."
Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy. ”

It seems clear that the main objective of the regulation is to give the data subject a high level of protection as long as it does not hinder the free movement of data. In most cases where there is doubt the regulation probably will be interpreted in the data subjects favour to comply with its objectives. However, since the free movement of personal data also constitutes an objective, if the regulation would be too strict towards the actors in a way that indirectly would hinder the free movement of data within the union both objectives would have to be weighed against each other.

Synopsis

There are two main objectives to consider when analysing the GDPR. Firstly, the protection of the rights and freedoms of natural persons and secondly the free movement of personal data. These interests need to be put in relation to each other to achieve a balance.

With the objectives of the regulation in mind the next chapter will look at how the GDPR and the directive defines the processor and controller and the interpretation of the definitions in case-law.

---

10 http://ec.europa.eu/justice/data-protection/
Defining a processor

The definition of a processor remains largely the same in the new regulation and the directive.\textsuperscript{11} Since the definitions remain unchanged, the case law that has précised the definitions should be going in to the new regulation. In this chapter the definitions in the new directive will be given as well as relevant case law to give said definitions context and by doing so create a clear picture of what constitutes a processor.

According to the new regulation a processor is “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.\textsuperscript{12} This gives two main criteria to constitute a processor. The first criterion is positive in the form of processing personal data. The second criterion is negative in the form of not being the controller.

Processing of personal data

Processing is defined as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means”.\textsuperscript{13} The scope of what constitutes processing is huge since it covers every operation. This means that not only sorting and structuring personal data is considered processing. Storing or transferring the information without any connection to it also constitutes processing.

Personal data is defined as “any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly”.\textsuperscript{14} The definition covers a lot of information since it’s not only direct information relating to an identified person. Information that indirectly can identify someone could be a surname in combination with a picture which by itself may not have been regarded as personal data.

Case law regarding processing and personal data

C-101/01 Lindqvist

The Court of Justice (“CJEU”) answered questions related to what constitutes personal data as well as processing. A person, Lindquist, had created a webpage which partly consisted of information about her co-workers. Regarding the information posted the Supreme Court

\textsuperscript{11} Directive 95/46 Article 2.
\textsuperscript{12} GDPR Article 4 p. 8.
\textsuperscript{13} GDPR Article 4 p. 2.
\textsuperscript{14} GDPR Article 4 p. 1.
established that a name in conjuncture with a phone number, working conditions or hobbies makes out personal data\textsuperscript{15}. Regarding loading the information on to a web-page the Supreme Court found that the procedure had to be considered processing.\textsuperscript{16}

The result can be seen as obvious but it shows that basically all information that can be related to a natural person is to be personal information.

\textit{C-70/10 Scarlet}

In their decision, the court of justice had to establish how broad the definition of personal data is to be. A company that represented copyright holders wanted an internet provider to set up a system in which they could filter out the users who used file sharing programs. The court had to determine whether IP-addresses constituted personal data.

Since an IP-address can be directly related to the user and their internet activities it constitutes personal data.\textsuperscript{17}

This case goes to show that even a string of numbers which by natural means cannot be related to natural person still constitutes personal data if it is possible to make the connection to a natural person. This broadens the definition greatly since as long as there is a key to connect the information to a natural person it does not matter if only some have access to said key it still constitutes personal information.

\textit{C-212/13 Rynes}

The case applies both to the definition of personal data and processing. A family had installed security cameras in their house which recorded the entrance to their house as well as the house opposite to theirs. Subsequently the camera recorded culprits. The court of justice had to decide on whether the recording constituted processing of personal data.

The court found that the image of a person is to be seen as personal data and to store and record said pictures constitutes processing of personal data.\textsuperscript{18}

This case shows that the threshold for processing is low since just recording pictures constitutes processing.

\textit{C 615/13 Client Earth}

\textsuperscript{15} C-101/01 Lindqvist p. 27.
\textsuperscript{16} C-101/01 Lindqvist p. 26.
\textsuperscript{17} C-70/10 Scarlet p. 51.
\textsuperscript{18} C-212/13 Rynes p. 22-25.
This case applies to the definition of personal data. The court of justice had to establish whether comments made by experts were to be seen as personal data, if the comments could be connected to the expert. A European agency, working with the risks involved with the food chain, established a report. In the report, some external experts made comments which affected the report. The agency would not disclose the information about which expert that had made certain comments due to it being personal information.

The court found that comments made by an expert are personal information. The circumstance that the comment is made in a professional environment does not change that fact. An individual agreement to disclosure of personal data does not take away that the information constitutes personal data.\(^{19}\)

This case goes to show that the trait of personal data does not change if it is established in professional environment. If the data falls under the definition of personal data, it retains that attribute.

_C 131/12 Google:_

This case relates to the definition of processing. The question raised was if the procedure used by search engines in which they gather information on the internet, filter it through their indexing programs and give the user a relevant result was to be seen as processing.

The court found that if the information is personal data, said procedure constitutes processing\(^ {20}\).

It was clear before the case that putting information on a webpage is processing. This case widens the definition, now it is enough to manoeuvre information that someone else has put on a webpage to fulfil the requirements of processing. Furthermore, it does not matter if one is aware that a part of the data processed is personal or not for the regulation to apply.

**The controller**

To define a processor, it is first necessary to define a controller. The definition of a controller is largely tied to the connection an actor has to personal data and if it in its connection decides how the personal data shall be processed. The definition of a controller is:

> "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; where the purposes and means of such processing are

---

\(^{19}\) C 615/13 Client Earth p. 30-31.

\(^{20}\) C 131/12 Google p. 28.
The negative criteria of not being the controller are based on the relationship between the controller and the processor. There always must be a controller, a part that actively decides to collect or use certain personal information. The controller decides what type of personal information that is used and how to use it. The processor takes a more passive role in that it only handles the information on behalf of the controller, that is usually the sole relationship between the parties.

This means that the processor often has little or no relationship to the information it stores. A typical example is a cloud service that lets a controller store data on their servers. Since they store the data on their servers they process the data but it is not particularly important to them what information the controller chooses to store.

Just because one part has more power over how information is handled does not mean that the part with lesser power cannot be a controller as well. It comes down to who determines the purpose and means of processing. There can be several controllers in relation to the same data if each of them fulfils the criteria of being a controller.

**Case law about the definition of the controller**

*C 131/12 Google*

The circumstances of the case were given in the case law regarding the definition of processing. The court also answers the question if the service of providing a search engine makes the provider a controller.

The court finds that, even if the search engine does not post information on a website the provider of the search engine still determines the purposes and means of processing within the activity of indexing and filtering information on the internet. The definition of a controller should be broad to ensure protection of the data subjects.

This case is interesting for the definition of a processor. It shows that it does not take much to be regarded as a controller. However, the search engine is directly accessible to the user and, by extension, the personal data the search engine makes available too. If the data would not have been accessible for the end user Google would probably not have been seen as a controller.

---

21 GDPR Article 4 p. 7.
22 GDPR. Article 4 p. 7.
23 C 131/12 Google p. 40-41.
Synopsis

The definitions of *processing* and *personal data* are wide. Basically, any information that can be connected to a natural person makes out personal data. It does not take much in the way of activities with said data to constitute processing. As seen in the case law the court of justice intends for the definitions to be broad to ensure a high level of protection for the data subjects. This is in line with the objectives of the regulations. However, the interpretation of a *controller* is also wide which makes the relevant area for this work, the processor, smaller. Even though an actor can be regarded as a controller without being the origin of the information, as Google, there still are a lot of activities that do not determine the means and purposes of processing but still constitutes processing.

Storing data on behalf of a controller that has constant access to the data and chooses what kind of data that is being stored should be the typical example. Those actors will be covered by the positive criteria while not being covered by the negative criteria.

With the amount of case-law that is centred on what should be considered a controller one can draw the conclusion that the courts as well as legislator have put weight in to the definitions. However, the definition only becomes relevant depending on the connection between the definition of the actors and the responsibilities tied to said definitions.

In the following chapters the responsibilities and the liability under the directive as well as the new regulation will be studied focusing on the responsibilities of the processor while also, in relevant areas, covering the responsibilities of the controller.
Responsibilities of a processor under the directive

Before analysing processors under the new regulation, the responsibilities under the directive need to be studied to put the new regulation in to perspective. The controllers’ responsibilities need to be covered to the extent that they are relevant to understand the processors responsibilities.

The directive is structured around the controller as the responsible actor. This chapter will look at the demands set on the processor through the controller. The controllers’ responsibilities will be covered briefly. Since the liability for processors basically stems from the contract with the controller a standard will be studied as well as contracts from some of the big actors.

Regulated demands on the assignment of a processor

The directive sets up some basic criteria for appointing a processor. The controller shall only choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures. Since the article is directed to the controller it is the controller who needs to asses if the processor meets the basic demands.

The processor must through the contract with the controller guarantee compliance with national data protection law which are based on the Directive. Also, there must be a binding written agreement which shall stipulate that the processor only acts on the controllers instructions and must ensure the security of the personal data it processes.

Regulation concerning confidentiality is directed to the controller as well as the processor and stipulates that anyone who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law. The confidentiality is tied to the controllers’ instruction so even if the article is directed to the processor too it still is the controller that largely sets the level of confidentiality in processing. And as will be seen below, the controller is the party liable for noncompliance.

The directive in a sense regulates some responsibilities for the processor but only indirectly through the contracts. The article is directed to the controller and empathizes that the controller chooses a suitable processor.

---

24 Directive 95/46 Article 17 p. 2
25 Directive 95/46 Article 17 p. 3
26 Directive 95/46 Article 16.
Liability

According to the directive *any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.*\(^{27}\) The processor is not mentioned at all in regards to liability. The person with the right to compensation must turn to the controller to be compensated even if the processor may be a better target for receiving adequate payment. There is no hindrance for the controller and the processor to contractually regulate the liability between each other. However, even if the controller can receive restitution from the processor contractually, that does not affect the data subjects’ possibilities to receive compensation.

When it comes to sanctions the directive leaves it up to the member states to implement suitable measures to ensure compliance with the directive.\(^ {28}\) The sanctions can therefor vary between different member states as long as it upholds the purpose of compliance with the directive.

In Sweden, the legislator has implemented fines.\(^ {29}\) The supervisory authority shall give the controller notice that if they do not comply with the regulation they are at the risk of fines. The controller shall have the right to protest and in case of execution of fines the supervisory have to turn to the court to the provincial court for determining the execution of the fines.\(^ {30}\)

**Responsibilities of a controller under the directive**

This thesis is focused on the processors liability but to be able to put the liability in perspective something needs to be said about the responsibilities of the controller. These obligations will not be treated as thoroughly as the processors but will be covered in this section.

Since the controller determines the purpose and means of the processing they often have a relationship to the data subject in form of for instance a customer or an employee. With this follow obligations to comply with requests from the data subjects, like deletion of data, information and more. These will not be covered further since they do not apply to the processors role.

---

29 PUL 44-45 §§.
30 Petersson s. 193 ff.
The indirect contractual responsibilities for the processor have already been covered; of course, these apply to the controller too, but directly. The relevant article is quoted earlier in this chapter.\(^{31}\)

The controller must make sure that the processing is secure, whether so by his own means or by ensuring that the processor does so. Both technical and organisational measures shall be taken to fulfil the responsibility.\(^{32}\)

Generally, the controller needs to inform the data protection agencies before processing any personal data which means that they need to, in a sense, record their processing activities.\(^{33}\)

Besides the more specific obligations the controller has a general obligation to make sure that the provisions following the directive are upheld. This general obligation ties together with the liability, which also is general for the controller as noted earlier in this chapter. The controller is liable for damages suffered to any unlawful processing following the directive.\(^{34}\)

The controllers’ liability is not unconditional. If the controller can prove that it is not responsible for the event leading to the damage the damages can be partly or wholly exempted.\(^{35}\)

**Standard, ASP 06**

ASP 06 is a standard developed by the Swedish institution of software industry. The developer represents the suppliers which may result in the standard for some areas come across as a bit unbalanced. The range of services can vary but the common factor is that the services are provided through internet.\(^{36}\) The recipient should in most cases be a controller when dealing with personal data since they are the ones determining what and how data should be used in relation to the service provided. The supplier should mostly be a processor in the applications or storage is on their servers.

The standard does not regulate personal data protection specifically. When personal data is processed there needs to be adjustments to comply with the demands on the contract set in the

---

\(^{31}\) Directive 95/46 Article 17 p. 2.

\(^{32}\) Directive 95/46 Article 17.

\(^{33}\) Directive 95/46 Article 18.

\(^{34}\) Directive 95/46 Article 23 p. 1.

\(^{35}\) Directive 95/46 Article 23 p. 2.

\(^{36}\) Permeus s. 407.
directive. However, it does regulate the liability between the parties and that part should remain the same in cases of personal data.

The standard greatly limits the providers’ liability. Firstly, the amount that the provider can be liable for is limited to half of the yearly fee for the service.\textsuperscript{37} The standard stipulates that the provider under \textit{no circumstances} shall be liable for loss of data or the recipients’ liability towards a third person.\textsuperscript{38}

There are general contractual principles internationally which are applicant to the terms if they can be seen as unreasonable.

Later, in chapter \textit{contracts to limit liability}, the general contractual principles will be further elaborated upon.

The standard is very much in the benefit of the provider, or the processor, in the context of this work.

\textbf{Synopsis}

The directive is structured around the controller having a general responsibility to comply with the rules as well as a general liability while the processor only is liable toward the controller through the contract between the parties.

There are requirements on the contract between the actors and by that there will be responsibilities indirectly placed on the processor.

Looking at a standard for processing personal data the conditions set out are very lenient towards the processor. The liability is greatly reduced.

The controller can possibly end up in an awkward position if dealing with significantly smaller actors as processors if the liability or sanctions directed towards the controller cannot be compensated at a later stage.

The next chapter will look at the responsibilities for the processor under the GDPR.

\textsuperscript{37} Permeus s. 438.
\textsuperscript{38} Permeus s. 437.
Responsibilities of a processor under the new regulation

As seen in the previous chapter the directive was not directed to processors directly. The new data protection regulation will increase what is required of both controllers and processors to fulfil their responsibilities\textsuperscript{39} and the liability for not fulfilling the regulation will be considerably more impactful for the actors. Furthermore, the regulation is targeted at the processors directly.

There are two aspects that needs to be considered. Firstly, what is required of the processor to comply with the regulation and secondary the liability for not fulfilling said responsibilities.

It will still be the controller that determines what data that is processed otherwise the processor will be seen as a controller. However, with the new regulation there is partly the contractual obligations toward the controller that already to a degree were regulated in the directive but there’s also demands that are directly applicable to the processor disregarding the contract between the parties. In this chapter, firstly the articles targeted towards the processor will be covered followed by the contractual demands and how they correlate to the demands in precedent directive. Lastly the liability will be covered.

Security

For processing to be secure according to the regulation both the processor “\textit{should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk}”.\textsuperscript{40} Factors to take in consideration are inter alia the nature and purpose of the processing, the cost of implementation and the risk of different freedoms for natural persons being impinged. Examples of implementations are pseudonymizing and encryption of information, the actors’ organization to be able to keep ongoing security for the system and restoration in case of technical incidents.\textsuperscript{41} A process of testing the system as well as the organization around the system.

It’s hard to know if a system of processing is secure as there are no clear criteria. Practice will eventually clarify the level of security deemed appropriate for different types of information. Processing according to an approved code of conduct speaks for an adequate level of security.

Documentation

\textsuperscript{39} P. & D.P. 2012, 12(4), 3-5.
\textsuperscript{40} GDPR Article 32 p. 1.
\textsuperscript{41} GDPR Article 32 p. 1.
A controller must keep “a record of all processing activities under its responsibility”.\textsuperscript{42} The record shall contain information about the controller, the purpose of the processing, descriptions of data subjects and what type of personal data as well as the recipients of the information. All the above are records that always shall be documented. In case of third country transfers of data additional information needs to be recorded. Where possible the controller shall document the time limit for erasure as well as the technical and organisational security measures.

The processor also has an obligation to keep a record although not as thoroughly as the controller. The processor shall record information about themselves as well as every controller they process data on behalf of and the categories of processing carried out for each controller.

This obligation to keep a record where absent in the precedent directive. Documentation that had to be kept according to the directive correlated to what needed to be presented to the authorities in case of investigation. Of course, in a sense, this will also be true in the regulation since it’s the authorities that control the registration. Although the burden has shifted, the principle now is that the controller must show that they comply with the regulation by default while the directive stipulated that the authorities had to have a case against the controller. Documentation for the processor wasn’t covered in the directive at all instead that should have been covered by the obligation to set up a binding contract between the controller and the processor.

### Cooperation with the supervisory authority and reports

The processor \textit{shall cooperate, on request, with the supervisory authority in the performance of its tasks}.\textsuperscript{43} When the new regulation enters in to force the supervisory authority can turn directly to the processor and request cooperation. This means that the processor also has to have system in place to be able to corporate accordingly. How far the obligation to cooperate can be taken will have to be seen through practice.

Furthermore, the processor \textit{shall notify the controller without undue delay about after becoming aware of personal data breach}.\textsuperscript{44} The obligation to report is not towards the supervisory authority but needs to be done to the controller which in turn can report the breach to the supervisory authority. Even if the obligation is towards the controller the processor will need to have preparations in place to notice and communicate breaches.

\textsuperscript{42} GDPR Article 30 p. 1.
\textsuperscript{43} GDPR Article 31.
\textsuperscript{44} GDPR Article 33 p. 2.
Assignment of a data protection officer

The directive did not demand that the processor in any case had to appoint a data protection officer ("DPO") The new regulation demands that the processor appoints a DPO if the general demands for a DPO is met.\textsuperscript{45} The requirement of a DPO is depending on if the processing is carried out by a public authority, The nature and the scope of the processing activities or the scale of the activity. The rules about appointing a DPO is indifferent between the controller and the processor.

Regulated demands on the assignment of a processor

The structure of the contract and selection is very much the same as in the directive, however the demands on what contents that is required has increased with the new regulation.

Firstly, the controller, as in the directive, needs to make sure that the processor can guarantee processing in line with the regulation.\textsuperscript{46} The big difference from the directive lies in the demands on the contents of the contract. The contract between the actors should \textit{set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller}.\textsuperscript{47} This is a bit more specific than demands in the directive.

The regulation also goes further in exemplifying what the more general description above shall include. In the precedent directive security, confidentiality and compliance with the controllers’ directives were exemplified, this also needs to be part of the contract according to the regulation. The security by a reference to article 32 treated above in this chapter and the part about compliance is largely the same with the difference that the directives needs to be \textit{documented}. Confidentiality is placed in under the contractual demands instead of under an own article but still affects \textit{people authorized to process the personal data}.\textsuperscript{48}

The new information that needs to be included in the contract not found in the directive correlates to the demands that are set forth earlier in this chapter.

\textsuperscript{45} GDPR Article 37.  
\textsuperscript{46} GDPR Article 28 p. 1.  
\textsuperscript{47} GDPR Article 28 p. 3.  
\textsuperscript{48} GDPR Article 28 p. 3 b.
The contract shall stipulate that the processor *assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.*\(^49\) This content correlates to the controllers’ obligation to choose an adequate processor the difference being that the processor need to agree to being able to fulfil the responsibility.

A point closely related to the demands on the contract to regulate secure processing and assistance to the controller with request form data subjects, is that, the contract needs to stipulate that the processor shall *assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor.*\(^50\) Article 32 and 36 of the regulation is about secure processing and prior consultation from the supervisory agency. This demand on the contract, in difference from the earlier ones shall make the processor help the controller to fulfil their responsibilities following the regulation.

The obligation for the processor to keep documentation was treated earlier in this chapter. The contract also needs to consist of rules about the controllers right to insight in said documentation. The contract shall stipulate that the processor *makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller*\(^51\). Since the processor already needs to have documentation the main difference following the contractual demand should be to have a system in place and allow the controller to take part of said information.

The last thing that needs to be part of the contract is that the processor *at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.*\(^52\) This should follow of the general demand that the processor only shall process personal data in compliance with the controllers’ instructions, however, that personal data is deleted or returned need to be clarified in the contract.

**Liability**

---

\(^{49}\) GDPR. Article 28 p. 3 e.  
\(^{50}\) GDPR. Article 28 p. 3 f.  
\(^{51}\) GDPR. Article 28 p. 3 h.  
\(^{52}\) GDPR. Article 28 p. 3 g.
As seen in the earlier chapters the processor is only liable indirectly through the controller when not processing in accordance to the directive. In the new regulation, the processor will be directly liable.

The regulation stipulates that the processor is directly liable in two scenarios. Firstly, the processor can be held liable where it has not complied with obligations in the regulation specifically directed to processors.\(^53\) As seen above there are lots of rules in the new regulation that are directed towards the processor directly. In all these scenarios, the processor will also be directly liable.

The second scenario in which the processor can be held liable is where it has acted outside or contrary to lawful instructions of the controller.\(^54\) This can, in a sense, be compared to the responsibility under the directive where the processors liability was tied to the contract with the controller, the difference under the regulation being that the suffering party can turn directly to the processor.

Even though the liability is limited to said conditions it will cover a lot of situations since it is tied both to the processors contractual responsibilities as well as the rules in the regulation.

Beside the liability there is also sanctions in form of administrative fees that can be applied to controllers as well as processors. The fees can be as high as 20.000.000 Euros or 4 % of the total annual turnover.\(^55\) The sanction is set by the supervisory authority. Factors that affect the size of the fee are determined based on the infringement in question, actions taken to mitigate the data among other factors.\(^56\) The liability will be looked at closer in a later chapter.\(^57\)

**The responsibilities of a controller under the new regulation**

As in the previous chapter the controllers’ responsibilities that are relevant need to be considered for a full picture, although to a lesser extent than the responsibilities of the processor.

The controller still has a general obligation to make sure that personal data are being processed in accordance with the regulation and must furthermore demonstrate that they are doing so. The

\(^{53}\) GDPR Article 82 p. 2.

\(^{54}\) GDPR Article 82 p. 2.

\(^{55}\) GDPR Article 83 p. 5.

\(^{56}\) GDPR Article 83 p. 2.

\(^{57}\) See chapter, *Contracts to limit liability.*
liability is tied to the general obligation and the controller is therefore generally liable for not complying with the regulation.  

All the contractual demands in relation to a processor that was treated earlier in the chapter are of course applicable to the controller too.

The controller needed to keep a record under the directive too, indirectly through their obligation to report to the supervisory authority. In the new regulation, there will not be an obligation to report processing activities although there will be an obligation to keep a record following the same principles as the processor.

For security measures the controller still needs to implement organisational and technical measures to make sure that processing of personal data is secure. The new regulation exemplifies what these measures can consist of depending on circumstances, although the width of the obligation should remain about the same.

The controller will be obliged to report to supervisory authorities within 72 hours in the event of a security breach unless it is unlikely to result in a risk for the individuals’ rights.

The new regulation emphasises on measures taken before the processing of personal data occurs. The principles and obligations should be considered when planning processing or implementing new products. Actions taken should not be reactive but proactive as much as possible.

**Synopsis**

There are two types of obligations for a processor following the new regulation. Some articles are directly applicable while others follow from the requirements set out for the contract between the actors.

The controllers’ obligations are to some extent increased come the new regulation even if many of the areas already were covered in the directive. There still remains a general obligation to ensure compliance with the regulation.

---

58 GDPR Article 5.
59 GDPR Article 30.
60 GDPR Article 33 p. 1.
61 GDPR Article 25.
Processors will be directly liable towards data subjects if not complying with the regulation as well as running the risk of receiving sanctions fees from the supervisory authorities which can reach high amounts.

The contractual demands can to an extent seem unnecessary where the new regulation directly regulates the procedure but it serves a purpose by regulating the responsibilities between the parties. The possibility to indirectly make the avoid liability will be covered in a later chapter.

Seeing as the data subject can turn towards the controller or the processor to receive liability in combination with the increased requirements, particularly for the processor, creates a higher level of protection while putting higher demands on the controllers and processors.

In the next chapter will give a concrete example of how the GDPR can change the situation for a typical processor, the cloud provider.
An example, cloud computing

In this chapter the intention is to highlight the regulations and technical aspects that have been covered earlier in the thesis by a concrete example. Cloud computing has existed in different forms throughout the computing history as a way to make the use of resources and hardware more effective, however, during the last years the concept has been reaching new users and applications to an extent not seen before.62

Definition of cloud computing

The national institute of standards and technology has defined cloud computing as “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.”63

By using network technology, it is possible to only use the amount of space or services that is required for a specific task. Instead of investing in a server that will not be utilized fully the network makes it possible to pay for the usage of parts of someone else server to the extent that is needed. It transforms the procedure to a running cost instead of a fixed cost.64

An example, storage using cloud computing

Now let us look at how the cloud provider as a processor is affected under the directive. The contract will determine the responsibilities of the processor, it does not need to consider personal data at all if the user does not regulate it in the contract. The cloud provider can therefore have different levels and security and ways to store data depending on if the data constitutes personal data or not.

In case of a data subject suffering damage due to noncompliance with the directive the data subject would have to turn to the controller for compensation. The controller would then turn

62 Christner s. 10.
64 Christner s. 15.
to the processor if the processor is at fault and be compensated, based on the assumption that the actors have regulated the responsibilities between each other.

If the controller were to be insolvent there would be no way for the data subject to turn to the cloud provider for compensation.

Following the new regulation, the cloud provider and the user would have to enter into a contractual agreement as well. However now the demand is also directed towards the cloud provider as the processor. It must therefore either make sure that the data processed does not constitute personal data or enter into terms in accordance with the regulation with all users.

Now, if the data subject suffers damage corresponding to infringements of the new regulation the data subject could choose which party to target for compensation. Even if the controller were at fault, the data subject could turn to the cloud provider, which in turn would have to receive compensation from the controller. In many of these cases the cloud provider has no relation whatsoever to the data subject more than storing data containing information that can be associated with the subject.

**Synopsis**

This example shows the clear difference between the directive and the new regulation. The data subject was at risk of ending up in an awkward position when attempting to receive compensation according to the directive. Following the new regulation, it is the cloud provider as the processor, who risks being liable in cases where the controller may very well be at fault.

In the next chapter, there will be a more analytical view of the actors’ definitions and the corresponding responsibilities.
Processors, the new controllers

In this chapter the previous chapters will be tied together to give a picture of the changes and the role of the processor going in to the new regulation. Potential problems will be identified to which solutions will be addressed going forward in the thesis.

From the directive to the new regulation

As seen in earlier chapters there is, in the directive as well as in the new regulation, a clear distinction between who shall constitute a controller or a processor. The distinction is important under the directive since all non-contractual liability is centred on the controller.

Looking at the obligations for the actors under the directive there is a general obligation for the controller as well as a general liability. This general liability will still be present in the new regulation and, as should be, the controller is the main party responsible for overall compliance. The number of specific demands on the controller covers about the same areas but are in some cases extended or exemplified.

Under the new regulation, the processors on the other hand has had their responsibilities vastly increased. Even though there is no general liability some areas such as security, documentation, cooperation with supervisory authorities and assignment of a DPO will be directly applicable to the processor. The demands on the contract between the actors have also increased.

The contractual changes should not have that much of an impact; after all, the directive already regulates what was required of the contract between the parties even if the article is directed at the controller.

The combination of the new demands together with the processor being directly liable for noncompliance could be the more problematic. Of course, there should be a solid protection of personal data but the actors’ roles still must be considered when the level of liability is decided upon.

Processors by default do not have a relation to the data subject since it is doing the processing on behalf of another actor. The same goes for what kind of data that is being processed, in some cases the processor has a closer relation to the data, in other cases there is no relation to the data at all.
As seen, it is not always an easy task for the courts to distinguish between personal and other data. Of course, the same goes for the processor, still they are by default responsible to determine what kind of data they process without any contact with the relevant data subject.

Do the areas where the controller still has a vaster liability justify the distinction between controller and processor that has been emphasized historically, what areas are the controller exclusively liable for? Also, taking in to account that there are widely different ways to process data and by so relation to the data. Could there be a need to distinguish between different types of processors as well as between controllers and processors?

**Processor as the new controller**

Even if the responsibilities of a processor and controller will be closer to each other following the new regulation there still are areas where only the controller can be held liable, mainly areas that stem from the relation to the data subject that the controller often have.

Many of the areas where the responsibilities of the processor will be increased seem to have already been regulated contractually between the parties. This in combination with the differences that still exists should make it a bit of an exaggeration to claim that the processor as of the new regulation could be seen as a controller.

The general liability is still placed on the controller. There is a possibility for the processor to single out the areas that are directly applicable to them and comply with them. However, for the possibility to single out areas to be relevant it must also be possible for the processor to comply with said areas. After studying the possibilities to avoid liability a conclusion about the differences between a controller and processor and the level of liability can be drawn.

**The need for a new definition**

Processor has throughout the directive and going in to the new regulation been seen as one entity. The fact of the matter is that processors can have a wide variety of relation to the data that is being processed.

Some processors have a direct relation to the personal aspects of the personal data for instance companies doing market research on behalf of controllers. These actors are quite close to a controller since they treat the information on a higher level (More about this in the technical
and it makes sense that their liability is almost the same as the controllers. However, there are actors that only will process the data on lower levels, that only store the logical information which can unlock the personal part of the data. There should be as much need to distinguish between these types of processors from each other as there is to distinguish between a controller and a processor.

The regulation does not differentiate between the different types of processors. In the directive, the legislator seems to have pictured the processor as an actor that just store and provide data for the controller, naturally the level of liability is low. In the new regulation, the legislator seems to consider the processor as an entity closer to the controller and naturally the responsibilities and liability will be more extensive.

By distinguishing between different types of processors a lot of the problematic areas could have been avoided and the level of liability regarded as more reasonable.

The distinction could be made at what level the data is processed, in other words if the processor has access to the personal aspect of the data.

The regulation does not distinguish between different types of processors and the level of liability seen over the whole spectrum will be high. The processors will need to adjust to these increased demands disregarding the connection they have to the personal data.

If the liability would be tied to the level of connection the processor has to the personal data, it would also be possible for the processor to decide the level of liability relevant to them. This would mainly be possible through technical means in which the processor distances themselves from the personal data, possibly in a way that makes it technically impossible to interpret the personal aspect of the data.

**Synopsis**

This chapter analysed the roles of the controllers and processors in relation to their definition and responsibilities. It shows how the definitions remain largely unchanged while the responsibilities have been altered. The processors relation to the data can vary greatly and with the new responsibilities there could be a need to adjust the definitions.

---

65 See chapter, *Code to limit liability.*
In the following chapters this thesis will look at the processors possibilities to avoid or limit liability through means of contracts or technical solutions. After which the analyse in this chapter will continue considering said possibilities.
Contracts to limit liability

Contracts make out an important part of the directive as well as the new regulation. In the directive contracts constituted the entirety of the processors liability while they make out part of the liability in the new regulation. Could processors use contracts to avoid liability besides what is required by regulation? This chapter will try to answer that question by first studying the absolute requirements on contracts in the regulation followed by international contract law in relation to the regulated responsibilities of the processor that are not bound to the contract.

Since the regulation regarding liability and administrative fines differ they will be studied separately starting with the liability.

There are two possibilities to affect the liability by contractual means. Firstly, to avoid liability by indirectly regulating it, in other words the processor can receive compensation from the controller after first paying the suffering subject or the supervisory authority. Secondly there is also the possibility to avoid liability in the first place by not being regarded as responsible. Both situations will be looked at and the possibilities of them analysed.

Contracts in the regulation

The requirements on contracts set out in the new regulation as well as in the directive are centred on the processor asserting to comply with certain standards following the requirements. This makes a lot of sense in relation to the directive where processors were not directly liable.

Since the new regulation will make the processor directly liable in many scenarios there should be possibilities to use contracts to limit the liability. This is not regulated in the regulation and general contract law will have to be studied in relation to the rules about liability to find possible contractual solutions.

International standards

Since this thesis is studying the regulation independently from national law, national contract law will not be considered. On an international level the Institute for the unification of private law have developed standard principles for commercial contracts. In Europe, there is the Principles of European contract law as well as the Draft Common Frame of Reference.
Even if these acts constitute soft law they should indicate general contractual principles on the international plane that are relevant in studying the possibilities for controllers and processors to regulate liability.

**Freedom of contracts, unreasonable terms and the regulation**

It is considered a general principle of contract law that parties are allowed to enter into contracts with who they want and on what conditions they want.66 This basic idea should permeate contract law in most countries and on an international level.

In contrast to the principle that is freedom of contracts are the binding requirements that follow by law. It is naturally not possible for parties to agree upon something between themselves and by doing so ignore binding law.

Even if a contract is not illegal it can still be invalid due to the conditions set out in the contract being unreasonable.67 The different international instruments use different words but the context should be about the same. Circumstances to take into consideration are for instance the strength of the parties, the circumstances when the parties accepted the terms and an excessive advantage for one of the parties correlating from the terms.

**Liability**

The data subjects’ right to compensation as well as the supervisory authorities’ obligation to impose fines follow directly from the regulation.

Any damage suffered “as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered”68. The processor is liable “for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller”69. To fully disregard liability towards the data subject through contractual means is therefore not possible.

---

66 PECL 1:102, Unidroit 1.1, DCFR II-1:102. 
68 GDPR Article 82 p. 1. 
69 GDPR Article 82 p. 2.
Administrative fines are to be imposed by the supervisory authority.\textsuperscript{70} Since the supervisory authority is not a party in the contract it is not possible to ignore the fines through contracts between the actors. Contracts can however still be used to place the final payment of the fines between the parties and to comply with the conditions stipulating the indemnification.

\textbf{Indirectly transferring liability through contracts}

The regulation gives the data subject the right to seek compensation from whomever of the parties that they choose if there are several involved. If actors that according to the rest of the article are found “\textit{responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject}”\textsuperscript{71}. This responsibility cannot be disregarded based on contractual agreements; it would go against the binding law that is the regulation as well as regulate the options for a third person that never entered the contract.

The liability is not absolute as will be seen below.\textsuperscript{72} However, this chapter is about the possibility to indirectly solve the liability issues contractually. The situation when both a controller and processor (or several) are found liable for the same infringement is regulated in the regulation. When one of the actors has “\textit{paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2}”\textsuperscript{73}. This situation gets interesting since it, in most cases, correlate to actors that have a contractual relationship with each other.

The wording of the article gives the impression that it is a definite rule that the parties should pay their part of the liability as seen by the regulation. This should also be the case were the liability has not been covered in the contract. In most cases this question should, at least to some extent, be regulated in the contracts. Since it is an internal relation between the contractual parties after the data subject has been compensated, the \textit{freedom of contracts} should make it possible for the actors to ignore the paragraph.\textsuperscript{74}

\textsuperscript{70} GDPR Article 83 p. 1.
\textsuperscript{71} Regulation Article 82 p. 4.
\textsuperscript{72} See subchapter, \textit{liability}.
\textsuperscript{73} Regulation Article 82 p.5.
\textsuperscript{74} Regulation Article 82 p.5.
Exempt from liability

In the preceding chapter the possibility to indirectly place liability was studied, in this chapter the possibility to directly avoid liability through contracts will be examined. The liability is not absolute, “A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage”\(^{75}\).

This dispensation from the otherwise severe liability raises some interesting questions regarding the processor. Firstly, it should not be responsible for the event, read by itself it leads towards the conclusion that it constitutes some sort of force majeure; however, it must be read in accordance with the rest of the article. The processor is to start with only liable for obligations set on them for the regulation, so it’s in that spectrum that the event which leads to the exempt lies. What does not in any way responsible for the event mean in the context of the regulation? Secondly the processor can only avoid liability if it proves that it is not responsible. How vast is this burden of proof? And of course, can contracts be used to reach the exempt of liability?

To address the first question the comments to the regulation do not give further guidance to when an actor should be seen as responsible, although it stipulates that the *concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation*\(^{76}\). The comment is about the data subjects’ right to liability and even if the quoted sentence covers how broadly damage should be interpreted. The same reasoning should be applicable on the interpretation of when a processor can be found responsible.

The objectives of the regulation were covered in the first chapter of this work.\(^{77}\) The two factors that are to be balanced against each other is the data subjects right to protection and the free movement of personal data. In most cases the protection of the data subjects’ rights should be the most relevant. One can conclude that the “*any way responsible*” will be given a broad interpretation.

The second question is hard to answer before any decisions from the Court of Justice has set out. However, the word *proves* tend to set a threshold which is quite high. In the end, it will be a question about evidence valuation.

---

\(^{75}\) GDPR Article 82 p.3.

\(^{76}\) GDPR Reason 146.

\(^{77}\) See chapter, *Objectives and intentions of the regulation.*
The administrative fines

The rules regarding the administrative fines are structured differently than the ones concerning liability in damages. The fines are not directly tied to any damage suffered but rather to the gravity of each individual case, although damage can be part of the consideration. The regulation mentions several factors that should be taken into consideration when determining the severity of the infringement.

The factors are quite comprehensive and covers the severity of the infringement objectively as well as subjectively. There is also a general clause making it possible to take into consideration circumstances not correspondent to one of the specific factors. Specifically, the factors are:

“(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.”  

The criteria to determine the fines do not leave much room for contractual solutions except the last, quite general clause. If a controller guarantees certain aspects in the contract it should constitute a mitigating factor for the processor.

Even though each individual case need to be considered the regulation sets out guidelines for the consideration by categorizing infringements to different articles with different limits to the fines. This should, in a sense, display the legislators view of which infringements that should be considered most severe.

Indirectly transferring administrative fines through contracts

---

78 GDPR Article 83 p. 2.
79 GDPR Article 83 p. 4-5.
As said before since the supervisory authority impose the fines there is no way to contractually predetermine which of the actors that shall pay the fine. However, as with the liability, there should be no issue to regulate who should carry the final burden. After all it is an internal relation between the contractual parties. Regarding the administrative fines there are no regulation stipulating who shall bear the final burden of liability. As long as the contractual condition cannot be seen as unreasonable, indirectly placing administrative fines should not be an issue.

**Exempt from administrative fines**

To be exempt from administrative fines the processor would have to show that the administrative fine is not applicable. There is no exemption for administrative fines in the same way as there is for liability. Since the supervisory authorities decide upon the fees and they are a governmental body they must consider the rules that apply to such bodies.

There regulation sets some conditions for issuing administrative fines. “*The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.*” 

80 This limits an arbitrary use of the administrative fines but it does not seem to leave much room for the processor to actively limit their liability.

There seems to be no way for the processor to reach a point where it run no risk of administrative fines what so ever through contractual means. The processor would need to comply with the regulation fully which cannot be achieved by contractual means.

**The situation with the unknowing processor**

It is not always easy for the processor to know if it processes personal data or not, since data on a low level just consists of ones and zeros. This can create problematic situations since the processor is directly liable when processing personal data.

In this context, it would be important for the processor to be able to safely conclude when the processing is affected by the GDPR. Contractually it is possible for the processor to stipulate a term where the controller guarantees that the data being processed are not personal if the controller does not say otherwise. Would such clauses be effective?

80 GDPR Article 83 p. 8.
Regarding the administrative fines, it should affect the assessment concerning the character of the infringement. However, that is only one of many factors to be taken into consideration, there still is the risk of administrative fines. The supervisory agencies should mainly target controllers guaranteeing the absence of personal data.

In the case of liability, the clause would have to show that the processor not is in any way responsible. If such a guarantee would have been effective depends on how broad of an interpretation the Court of Justice gives the article. Most likely it will not be enough to completely avoid the risk.

Processors seems to run the risk of liability even when they are unaware that they process data that is not personal.

**Synopsis**

There are international principles and standards applicable to contract law. The principle of freedom of contracts should be considered as an international standard. This principle has to put in relation to the contract not being illegal or unreasonable.

The GDPR consists of certain requirements on contracts. Besides the absolute requirements there should be possibilities to limit the liability by regulating more than what is required.

Since the data subject or the supervisory agency who are to receive compensation are not contractually bound by the contract between the actors their right to receive compensation or conduct fines are not affected by the contract. It should however be possible to indirectly regulate the liability as well as limit the liability as well as the administrative fines.

This chapter looked on contractual solutions to avoid liability. The next chapter will look at how data is stored technically and try to find possible technical solutions.
Code to limit liability

When studying IT-law it is important to analyse the technical solutions in order to understand how the law shall be interpreted. The Internet as it is and how different applications work are not something that has to be but rather a result of architecture, architecture that can be changed in the same way as laws can be changed.\textsuperscript{81} In the case of data protection, data storage is the technical procedure that needs to be considered. In this chapter the basic concept of data and processing (typically storage) will be covered followed by an analysis of the possibility to adjust said system to comply with the demands set by the new regulation.

What is data in a digital environment?

As seen earlier in this thesis the directive and regulation defines personal data as any information related to a natural person. What should constitute the data part of the definition is information.\textsuperscript{82} Information is also the main factor in a more general definition of data, quantities, characters, or symbols on which operations are performed by a computer\textsuperscript{83}.

Then how is the information stored in computers? Computers use a binary system to store information. A binary system only consists of the numbers 0 and 1. By only using these two numbers the computer can interpret it as off or on. This binary information is then stored and from that basic information the computer can produce other numbers, letters, pictures and all sorts of utility.\textsuperscript{84} This is what is referred to when saying that information is becoming digitalized.\textsuperscript{85}

This data by itself, the binary numbers, consists of personal data when they after operations carry information related to a natural person. If said operations did not exist, the personal data could not form the information related to a natural person and should not constitute personal information.

How is data processed?

Processing is defined as any set of operations performed on personal data according to the regulation. Naturally it can consist of a lot of different procedures which in turn means that

\textsuperscript{81} Lessig s. 6.
\textsuperscript{82} GDPR Article 4 p. 2.
\textsuperscript{83} https://en.oxforddictionaries.com/definition/data
\textsuperscript{84} http://homepage.cs.uri.edu/book/binary_data/binary_data.htm
\textsuperscript{85} Siepel s. 25.
processors can constitute different types of actors. The first type that comes to mind is usually the data storage processor, for instance by a cloud service; they typically do not deal with the data in the form that present the personal part of the information while still carrying the pieces that together constitute that part of the information. Other actors deal with the information on a higher level and therefore the personal part of the data becomes more direct.

Data is mainly stored and achievable through databases. Databases are structures the data logically and makes it possible to access relevant data through set commands. One of the most common languages used today is SQL. With the use of databases it is possible to for processors that only stores data to make it available at a higher level and partake in the personal information if they choose to do so.

When a computer performs logical steps on information it can be called an algorithm. An algorithm is a series of predetermined operations on data that will guarantee the results set out to reach. The following section will look at cryptography, which often uses algorithms for encryption and decryption of data.

**Cryptography**

Cryptography is to transform information to a form that is unintelligible to persons who do not have the key to unlock the information. When encrypting data algorithms are used to modify the data and a corresponding algorithm is needed to receive the data in the same form. It can be seen as shuffling all the numbers following a set order. After the ones and zeros are shuffled it is not possible to get the information on a higher level. When using the right algorithms, the numbers get reshuffled to its original format and for instance a picture can be seen.

**Code required by the regulation**

According to the regulation the processor shall have appropriate technical implementations as part of the security requirements. The regulation exemplifies certain areas that should be covered.

“(a) the pseudonymisation and encryption of personal data;

---

86 [http://searchsqlserver.techtarget.com/definition/SQL](http://searchsqlserver.techtarget.com/definition/SQL)

87 Siepel s. 35.

88 Garfinkel, s. 193.

89 Garfinkel, s. 191 ff.

90 GDPR. Article 32.
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.’’

Encryption is part of what should be required for data to be considered secure. This should aim at the relevant actor encrypting data, meaning that the data is encrypted by the processor after receiving the data from the controller when applicant to the processor.

The other examples of what is required is quite general. They can be interpreted as having adequate systems in place technically as well as organisationally. How much is required by these systems will need to be established through case law.

**Code to limit liability**

Naturally the processor avoids liability per the technological responsibilities of the GDPR if instituting systems that comply with those demands. However, there are other sources of liability, can these be avoided by implementing adequate systems that are not directly required by law. To answer this the rules about liability and supervisory fines need to be put in relation to the technical aspects.

The liability in the regulation was covered in depth in an earlier chapter. To be exempt from liability a processor needs to prove “that it is not in any way responsible for the event giving rise to the damage”

Damage generally should stem from information about the data subject being leaked or published where it should not be. Adequate encryption should make it possible for the processor to avoid liability simply due to the fact that there will be no damage suffered.

Encryption does not contribute to cooperation with the supervisory agency, assignment of a DPO and documentation, but these responsibilities should not be such that noncompliance leads to a damage which is a requirement for liability.

---

91 See chapter, *Contracts to limit liability.*
92 GDPR Article 82 p. 3.
Technical aspects such as loss of data and responsibilities correlating to the quality of a service should already be considered by the processor since the controller can be eligible to compensation even in cases where data is not personal.

**Code to limit administrative fines**

The administrative fines do not correlate to the damage as the liability does. That means that the requirements on documentation, cooperation and assignment of DPO will not be met just by making the technical aspects secure enough so that the data subject does not suffer any damage.

When conducting the administrative fines the supervisory authorities will make a decision based on the individual case and several of the areas set out for the supervisory authority to consider when issuing fines can be catered to by technical implementations. Technical measures are directly mentioned in the article for determining the degree of responsibility placed on an actor. Implementing technical solutions should as well constitute an action to mitigate damage.

That being said, as long as a processor processes personal data there seems to be no way to completely secure themselves from supervisory fines.

**A working model**

When considering the technical possibilities to avoid liability one also needs to consider the cost and other affects the procedure would have to the service.

Operations such as encryption algorithms are usually quite effective, but it is still an extra operation that needs to be performed. If the operation is performed many times it will affect the required performance from the processor as well as the controller. What has made the use of external processors to an expanding market is largely the effective allocation of resources.  

If the system demands to much performance it will not be effective to use the services anymore and actors will once again store data locally.

**Synopsis**

93 See chapter, *An example, cloud computing.*
This chapter looked at the possibilities for the processor to limit liability using technical solutions mainly encryption.

Data is stored at logical level just using ones and zeros and by the use of databases and associated commands it is possible to receive relevant information from the cluster of logical information. A processor has access to the personal information even if they only store the data as long as they have the relevant commands.

Technical solutions can create a situation where damage and liability are unlikely. The solutions can also affect the supervisory agencies considerations when determining administrative fines. However, it should not be possible to completely exclude from liability or administrative fines using only technical solutions.

In the last chapter of this work conclusions will be drawn of what has been presented so far.
Conclusion

Can processors avoid liability using contracts or technical solutions?

After studying contractual and technical solutions in relation to the articles stipulating liability there does not seem to be a way to completely avoid liability by either of the methods. However, in practice the solution will not be found just using contracts or a technical solution, a combination of both would likely be used.

Encryption is a way for the processor to distance themselves from the personal aspect of the data. If the processor themselves encrypt the data, they will hold the key to unlock the personal information. If they receive the data encrypted it will not be possible for them to transform the logical information to personal information.

However, as it stands it is not relevant who holds the key, as long as there is a key the data is considered personal data. This means that the processor will be held liable as long as the data in the hands of anyone can be transformed to personal data. This condition was set out by the Court of Justice in relation to the directive and could need to be revisited with the increased liability of the processor.

Contractually the possibility to indirectly regulate the liability could be applied, however this is under the condition that the other party has sufficient means to cover the damages. In many cases the processor should be relatively large actors having access to huge server halls and storages of data. Compensation from a significantly smaller controller will not always compensate what has been suffered.

At this stage, it is hard to say how the supervisory agencies will apply the administrative fines in practice. It could be that certain levels of technical implementations and contractual guarantees will exempt processors from liability in practice. Just by the wording of the GDPR it seems that fines could be issued in many situations.

If the contracts where to be combined with the technical solutions, the processor could stipulate in the contract that the controller must notify the processor if the data constitutes personal data. In case of personal data, the controller or a third party specializing in encryption could encrypt the data before it reaches the processor. The processor now only stores data which cannot be

---

94 C-70/10 Scarlet p. 51.
put together in to any relevant information without the key. When the controller needs to access the data, the processor sends the encrypted information which the is decrypted and the controller can access the information.

This solution is not possible if the processor needs to deal with the personal aspect data. However, this would differentiate between the processors that are close to a processor in the way that they process the data to the ones that do not have a relation to the personal aspect at all.

The solution would also be performance effective in the sense that only data that are personal need to be encrypted based on the contractual guarantee and other data can be stored as is. This will not work while data constitutes personal data as long as there is key somewhere.

One big problem for the processor is that the regulation and the liability that follow is applicable directly if personal data is being processed. With the contractual guarantee mentioned above the controller would have to inform of what data is being processed. Such clauses should affect the degree of liability and supervisory fines. However, it will not exempt the processor from liability. The data subject has the right to compensation from whomever of the controller and the processor. Since such a clause likely will not exempt the processor from liability fully the situation ends up the same as placing liability indirectly. The processor must hope that the controller can compensate them at a later stage.

Interpretation of the supervisory agencies and case law will have to determine the processors possibilities to avoid liability in practice. As it stands it seems to no clear solution for the processor, not matter what level of processing, to completely exempt from liability.

**Considering possible solutions, are the definitions adequate?**

This work will now return to the analyse of the definition of the actors earlier in this work\(^95\) adding the dimension of possibilities to avoid liability.

The conclusions made earlier seem to be consistent when considering the possibilities to avoid liability. The difference between a controller and a processor is still relevant, it is possible for the processor to single out and comply with the rules that are directly applicable.

---

\(^{95}\) See chapter, *Processor, the new controller*. 
The issue remains that the processor can be vastly different entities. This leads to the possible solutions studied above, like encryption, cannot be utilized to effectively avoid liability.

If the regulation would differentiate between processors based on which level the data was accessible to them and regulate liability accordingly the processors without a relation to the personal information would be directly exempt from relevant liability. If the regulation would differentiate between processing personal data and just data based on the possibility to access the personal information it would be possible for processors to exempt themselves indirectly using encryption.

The definitions were created in relation to the directive, the structure of the legislation will change with the new regulation. To just take definitions built around another system and place them in to a new set of rules can result in problems and as it stands the definitions seem to be insufficient.

**Considering possible solutions, is the level of liability reasonable?**

The main objective of the GDPR is to give natural persons a high level of protection in regards to personal data. Mainly by harmonizing the rules by regulation and by increasing the responsibilities of the actors. For a new regulation to be implemented the legislator must have considered the precedent directive ineffective.

The structure of the directive where the controller was the only part responsible for the noncompliance would seem to be lacking. The limited possibilities for data subjects to receive compensation from a processor who is at fault needed to be adjusted.

With the new regulation, it seems as the legislator completely tipped the weights by making all types of processors directly liable for not complying with the rules that are directed towards them.

Even if a high level of protection for the data subject is something desirable, too strict rules all over the board will result in services not being as effective or supply decreasing. There is a reason for the increased use of external services, it is an effective way of allocating resources, both from the perspective of the supplier and the receiver the service.
The levels of liability that will be in the directive seem to be directed towards a processor that processes data in a way that is close to that of a controller. There is however a whole spectrum of processors and in regards to many of these the liability seems to be too strict.

Had there been a clear way for these actors to exempt from liability it could seem reasonable. However, as it stands not only is the liability high but there is no way to safely avoid the administrative fines or the liability.

**Synopsis**

To answer the questions set out at the start of this work. The processor will be directly liable in specific areas following the new regulation. There is no general liability for the processor. However, many of the areas where the processor can be liable are huge and the areas where the processor by default is exempt from liability are mainly areas connected to the relationship with the data subject.

The definitions seem to be lacking in the new regulation. The actors were defined to a set of rules structured around the controller being the only party liable. With the new regulation and the increased responsibilities for the processor as well the different types of processing possible it seems odd that the same definitions should be applicable. To just put said definitions in to another legal structure leaves the definitions wanting. Mainly the definition of the processor should be considered redefining due to the changes facing the role as a processor.

As it stands there is no clear way for the processor to exempt from liability either through contractual, technical means or the combination of the two. There are possibilities to limit the liability based on the considerations made when issuing fines or liability.

The increased liability will most likely increase the rights of the data subjects. Even considering that, the extent of the liability seems to be unreasonable. The liability would seem reasonable if only applied to certain processors, but when applying it to all processors, no matter the nature of the processing it cannot be seen as reasonable.

This being said, practice and implementation of the regulation will determine the effect the liability will have on the actors, the protection of the data subjects and the market as a whole.
Summary

25 May 2018 the new data protection regulation will enter in to force. There has always been an important distinction between the controller and the processor in European regulations regarding processing of personal data. The distinction will be largely the same going from the precedent directive to the new regulation.

In the directive, the controller, as the actor that determines the means and purposes of processing was liable. The responsibilities in the directive were written towards the controller and suffering parties were directed to the controller. If the processor was at fault the controller had to seek compensation from the processor on contractual basis.

In the new regulation responsibilities are in many cases directly turned towards processors. Areas such as security, documentation, cooperation, data protection officers and contractual demands will apply to the processor as well. In case of a data subject suffering damage due to data not being processed in accordance with the regulation the processor will be directly liable. There will be administrative fines issued by the supervisory authorities’ that can amount to large sums. The controller will largely be responsible for the same areas, although some of said areas demand more of the controller.

The distinction between a controller and a processor will still serve a purpose. The controller is still the only actor that has a general liability and is responsible for areas correlating to the relation to the data subject. In that sense, there still is a difference between the actors. A processor can vary to a large degree from either only storing data to working with the personal information directly. This could warrant a distinction between processors as much as the distinction between the controller and the processor.

Two ways for the processor to avoid or limit the liability could be through contracts or technical solutions.

The regulation requires certain areas to be regulated in contracts. However, there could be room to address liability contractually where not required. Contractual principles set out internationally must be considered in relation to the regulation. There is no way to exempt fully from liability or liability using contracts. There are possibilities to affect the considerations made when issuing either administrative fines or liability. The actors should be able to regulate the liability indirectly between each other.
Data is stored as ones and zeros in computers this information can then through the use of logical commands and databases form information that is intelligible. Using cryptology data can be put in a state where it is not possible to transform in to an intelligible form without a key to decrypt the data.

There are technical demands set out in the regulation. The possibilities to go further than what is required to exempt from liability is limited. Mainly due to personal data being considered personal no matter if it is encrypted and can only be unlocked by another party. As for contracts, there are ways to limit the liability using technical solutions. Damages should basically be non-existent if the security is high enough and the data is encrypted.

The new regulation seems to hold processors liable to an unreasonable level considering that the definition of a processor comprises all types of processing. From the directive, not achieving sufficient protection of the data subjects it seems as the processor will be held liable for areas they in many cases cannot affect.
Sources

Regulations

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

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) [.cit GDPR].


Soft law

UNIDROIT PRINCIPLES OF INTERNATIONAL COMMERCIAL CONTRACTS [ .cit Unidroit].

Principles, Definitions and Model Rules of European Private Law [ .cit DCFR].

Principles of European Contract Law [ .cit PECL].

Literature

Permeus, Andreas, Lindberg, Daniel. 2013. IT-avtal, en kommentar till IT-branschens standardavtal, Jure Förlag AB. [.cit Permeus].


Petersson, Roger, Reinholdsson, Klas. 2007. Personuppgiftslagen i praktiken, 4 u, Nordstedts juridik. [.cit Petersson].


**Case-law, European Court of Justice**

C-101/01, LINDQVIST, 6.11.2003. [ .cit C-101/01 Lindqvist].

C-70/10, SCARLET EXTENDED SA V. SOCIETE BELGE DES AUTEURS, COMPOSITEURS ET EDITEURS SCRL (SABAM), 24.11.2011. [.cit C-70/10 Scarlet].

C-212/13, RYNES V. ÚŘAD PRO OCHRANU OSOBNICH ÚDAJŮ, 11.12.2014. [ .cit C-212/13 Rynes].

C-615/13 P, CLIENT EARTH ET AL. V. EFSA, 16.7.2015. [ .cit C-615/13 Client Earth].

C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014. [ .cit C-131/12 Google].

**Articles**


**Other sources**


[https://en.oxforddictionaries.com/definition/data](https://en.oxforddictionaries.com/definition/data) (Oxford dictionary definition of data)
http://searchsqlserver.techtarget.com/definition/SQL (Techtarget on databases and SQL)

http://homepage.cs.uri.edu/book/binary_data/binary_data.htm (Data on a lower level)

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (National institution of standards and technology, definition of cloud computing)