UiO : Faculty of Law
University of Oslo

An implementation assessment of the general data protection regulation

A practical study on data protection within the financial market in Luxembourg

Candidate number: 7005

Submission deadline: 01.12.2018

Number of words: 15.033

Table of contents

Foreword

Working for a consultancy firm on the implementation of the GDPR with various clients is a tremendous and exciting experience that I have the chance to have since mid-2017 until now. During my years of studies when we were analysing the draft of what will become the GDPR, it appeared to me as a comprehensible regulation compared to other extremely complex European texts. However, back then, I would not have known the complexity and the difficulty of the GDPR that reside in its implementation. The GDPR is a fascinating text that has entered into force in 2018, twenty-three years after the last European Directive of 1995[1] when Google did not exist yet. This is where the subtilty of the GDPR lies, the regulation is not only related to the processing of personal data on the internet with a systematic collection of data as we have all faced, the GDPR is regulating the processing of personal data both electronically and on other supports – such as paper. This is a concept that had to be explained and discussed thoroughly with my clients during the course of the GDPR's implementation projects. The personal data that is collected and stored on the various software platforms and IT systems that a bank uses is actually most probably not where the focus is. The focus is on all the personal data that is collected on paper, and that is stored in folders in an unlocked drawer for an unlimited period of time, because we forgot about them. There is a considerable chance that in this folder there is the resume of an employee who provided it during the hiring process six years ago, who succeeded and was hired and has also resigned since. Is the personal data on the resume in the dusty folder accessible to every employee of the company up-to-date and necessary? No. However it may cause damage to the data subject if the resume is circulated or misused. In all honesty, in my professional experiences I have shortened and most probably popularised the definition of the GDPR to explain it to my clients. I have told them that the GDPR is simply a way to clean up their drawers, their IT systems and computer drives, in order to collect and to keep solely the personal data that is necessary, but also to implement procedures and review processes to ensure that it remains that way, and that in case of a data breach occurs they know exactly who is concerned, what is affected and how big the damages may be. Therefore, in theory, the GDPR could be considered as straightforward. The difficulty of the practical implementation of the regulation is that GDPR requires a lot of practical processes implementation, where it does not provide much details on how to achieve this compliance. This where the Working Party 29 and the now called European Data Protection Board[2] are having a major and necessary role to guide the businesses in their implementation of the GDPR. This is also a role that several data protection national authorities have taken up with the development of their own guidelines and methodologies that are used across the European Union, such as the guidance of the UK ICO and the French CNIL.

[1] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[2] https://edpb.europa.eu

The understanding of the regulation and the integration of the changes into operations is a difficulty that all businesses in Luxembourg are struggling with regardless of their size and their sector, from international asset managers to manufacturing companies. It is from practicing and working together with those stakeholders in the context of my day-to-day activity that my interest for the GDPR has increased and spread to eventually become the obvious topic to discuss for the closure of my LL.M. at the University of Oslo.

As a consultant assisting clients to comply with the European and national laws and regulations, the present paper describes how I transitioned from the theoretical analysis of the text to the practical implications and applications of the European General Data Protection Regulation ("GDPR"). This is due to me accompanying many clients in their day-to-day implementation and the integration of the published changes into operations. The views and opinions expressed herein cannot be construed as advice and are to be understood only in the context of the present paper. No third party can be held liable based upon these opinions.

Introduction

In April 2016, the European Parliament intended to strengthen and to unify the data protection in the European Union by implementing a new regime in the form of the General Data Protection Regulation 2016/679 (hereinafter "GDPR"). As GDPR entered into force in May 2018, national authorities throughout Europe have begun to adjust their legislation in order to provide some specific industries with particular guidance on ensuring data protection. One of the business sectors that is impacted by the requirements of data protection legislation is the financial sector and its different stakeholders. The financial sector is an industry that is being heavily challenged by the extensive European efforts of regulating, it has been modelled and re-modelled from various angles during the past years with the UCITS V directive[3], AIFM directive,[4] EMIR regulation[5], MiFID,[6] MiFID II[7] (altogether the "Financial Regulations"). In addition to ensuring the compliance with the specific regulations for its sector, the financial industry has to ensure the conformity of its stakeholders with the more generally applicable European regulation such as the GDPR. This need to satisfy the requirements from vastly different legal frameworks is one of the challenges that the financial industry is facing today.

Luxembourg is the second largest investment fund centre in the world and the financial sector is the largest contributor to the Luxembourg economy. In addition, Luxembourg has a particular focus on data protection evidenced by the fact that some of the requirements outlined in the GDPR were already introduced in Luxembourg with the law of 2 August 2002 on the protection of persons with regard to the processing of personal data (hereafter the "Law of 2002")[8] and with the law of 30 May 2005 providing specific provisions with regard to the processing of personal data in the electronic communication sector (hereafter the "Law of 2005")[9]. For those reasons, the choice of Luxembourg to focus a study on both the financial market and the data protection is indisputable. The data protection is a topic that is approached by two intertwining perspectives – the data subject perspective and the business perspective, as data protection involves many requirements that businesses need to tackle in the course of the good conduct of their activities. The development of the analysis hereunder focuses on the business perspective of the data controllers and therefore, unless specified otherwise, any reference to a company implies that the company acts as data controller for its data subjects, being its employees, its clients and its contractual parties. In the below assessment, "data subject" may refer to all the previously mentioned.

3 Directive 2014/91/EU
4 Directive 2011/61/EU
5 Regulation 648/2012
6 Directive 2004/39/EC
7 Directive 2014/65/EU
8 https://cnpd.public.lu/content/dam/cnpd/fr/legislation/droit-lux/doc_loi02082002_en.pdf
9 https://cnpd.public.lu/content/dam/cnpd/en/legislation/droit-lux/doc_loi30052005_en.pdf

Luxembourg has a data protection authority, the Commission Nationale de Protection des Données (hereafter the "CNPD"), that is a rather small organization composed of thirty people and which is tremendously expanding its resources. Still, regardless of the current limited size of its workforce and due to the favourable small size of the country of Luxembourg and in line with a lengthy history of practices, the CNPD has the ability to work closely together with professionals of the financial industry to develop its guidance and directives in light of the GDPR. The fact that the Law of 2002 and the Law of 2005 are already partially implementing the high level of protection issued by GDPR gives an insight on the advancement of Luxembourg in the matter of data protection. Even if data protection is not a recent topic in Luxembourg, the requirements provided in the new regulation with regards to the effort of documentation and required assessments are unfamiliar for both the national authority and also the stakeholders of the Luxembourgish industry. For those reasons, this paper is oriented on an analysis of the practical implications of the GDPR with a focus on the country of Luxembourg and Luxembourgish industries under both the national Luxembourgish legislation and the European legal framework.

1 Chapter 1: A practical analysis of data processing under GDPR

1.1 Section 1: The ex-ante risk-based approach

1.1.1 The ex-ante framework definition

In line with the terms of the Recital 90 of the GDPR, the data protection impact assessment (hereinafter the "DPIA") shall be carried out prior to the data processing. Therefore, a company needs to implement a systematic control to ensure that every new data processing is assessed prior to its application. Each stakeholder of a company that may be the sponsor of a new project involving a new data processing or who is implementing a new data processing shall conduct a data protection impact assessment prior its execution. Performing a data protection impact assessment should run easily once the proper methodology has been defined by the company through its data protection officer (hereafter the "DPO") or the person in charge of data protection in the firm. However, empowering the stakeholders of a company that are at the heart of the development of each project might raise difficulties. For this purpose, a company has to raise awareness on data protection amongst the heads of its departments and also establish controls ensuring that a data protection impact assessment is systematically conducted on new data processing.

As an example, it has been seen that companies have introduced data protection in their project methodology guidelines. Therefore, data protection is an aspect that any new project should cover and that will be discussed by the decisional organ of the company at the same level as other project management topic such as costs for the company, IT systems impacted, potential financial or time gain for the company. Where the new project may introduce a new data processing, the project manager or the sponsor informs the DPO or the person in charge of data protection, and they will work together to perform the data protection impact assessment.

Consequently, the data protection impact assessment is at the heart of any new project of a company and is conducted not solely by the DPO but by the person of the business line knowing the project acutely. Furthermore, where the DPO is involved in the development of a new project or change in the company, he may identify additional new data processing which should be assessed prior the implementation of the project. The DPIA is a major part of any project as the results of the assessment will then be addressed with the implementation of measures in line with the data privacy by design and by default principle *(see Section 2).*

1.1.2 The two-step impact assessment

1.1.2.1 The determination of the activity requiring the performance of a DPIA

According to the Recital 84 and the Article 35 of the GDPR, when a processing operation is likely to result in a risk for the rights of the data subject, the data controller shall perform a DPIA to evaluate the origin, nature, particularity and severity of this risk.

In this context, conducting a DPIA is not mandatory for all the data controller's operations or activities, but solely for the processing operations that the data controller has identified as likely to result in a risk for the data subject and his rights. Therefore, the GDPR requires from the data controller in a first instance to assess whether its operation is likely to result in a risk for the data subject; and in a second instance to perform the DPIA when it is necessary. The DPIA as defined in the Article 35 of the GDPR appears to be then a second step in the process of the overall assessment of the data processing's risk.

Considering that personal data is "any information relating to an identified or identifiable natural person who can be identifiable directly or indirectly"[10], the GDPR in Article 34(3) outlines three criteria to consider for the assessment of the likelihood of a processing activity to result in a risk for the data subject, "(i) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (ii) the processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; (iii) or a systematic monitoring of a publicly accessible area on a large scale."

In addition to the regulatory criteria, the CNPD, as required under Article 34(4) of the GDPR has published a list of criteria complementing the requirements outlined in the GDPR. Therefore, a processing operation shall be considered as likely to result in a risk for the rights of the data subject when (i) datasets have been matched or combined, (ii) the data processed concerns vulnerable data subjects, (iii) an innovative use of personal data or application of technological or organisational solutions, (iv) when the processing in itself prevents data subjects from exercising a right or using a service or a contract[11].

[10] Article 4(1) of the GDPR

[11] https://cnpd.public.lu/content/dam/cnpd/fr/actualites/national/2018/formation-cnpd-intro-pd/en-3-obligations-du-rt.pdf

Besides the provision of additional criteria, the CNPD extends also the scope of the criteria defined in the GDPR by specifying that a processing operation shall be considered as likely to result in a risk for the rights of the data subject if the processing is a systematic monitoring of data subject, regardless if the monitoring concerns a publicly or non-publicly accessible area or is the systematic monitoring is performed on a large scale. Furthermore, the CNPD considers that any processing of sensitive data is likely to result in a risk for the data subject without considering if the processing is performed on a large scale, and it considers that any processing performed on a large scale is considered as likely to result in a risk regardless the data processed qualifies as sensitive data or not. As a consequence, with the provision of the above-mentioned additional criteria, the CNPD enlarges the scope of application of Article 35 of the GDPR and tends to induce that the DPIA shall be conducted systematically.

1.1.2.1.1 Article 35(1) – conduct of a pre-assessment

The execution of a DPIA is not mandatory for a data processing operation that does not enter into the scope of the regulation nor into the scope of the criteria as defined by the national authority. However, to determine whether they shall conduct a DPIA for a data processing, data controllers shall initially perform a pre-assessment to assess whether a data processing is likely to result in a risk for the data subject. In a first instance, in order to perform a pre-assessment, data controllers have to implement a methodology to carry out the pre-assessment and to ensure that systematically, new data processing operations are analysed and that existing ones are reassessed on a regular basis. The determination of the pre-assessment may be as cumbersome as the determination of a DPIA, as it requires an analysis of the data processing in light of all the criteria previously defined (see Section 2.1.a). In a second instance, following the result of the pre-assessment, data controllers decide to conduct or to not conduct a DPIA on the data processing. In order to substantiate the representation of this pre-assessment in the DPIA process for the purpose of this paper we outlined it in red in the chart hereunder of the WP29. Where the data controller makes the decision to not conduct a DPIA on a data processing, he shall be able to evidence that this is the result of the pre-assessment that he conducted. Where the controller fails to evidence that he performed this pre-assessment and where a data breach occurred on the specific data processing operation, the controller is failing on his obligation and he may be subject to an administrative fine according to the Article 83 of the GDPR.

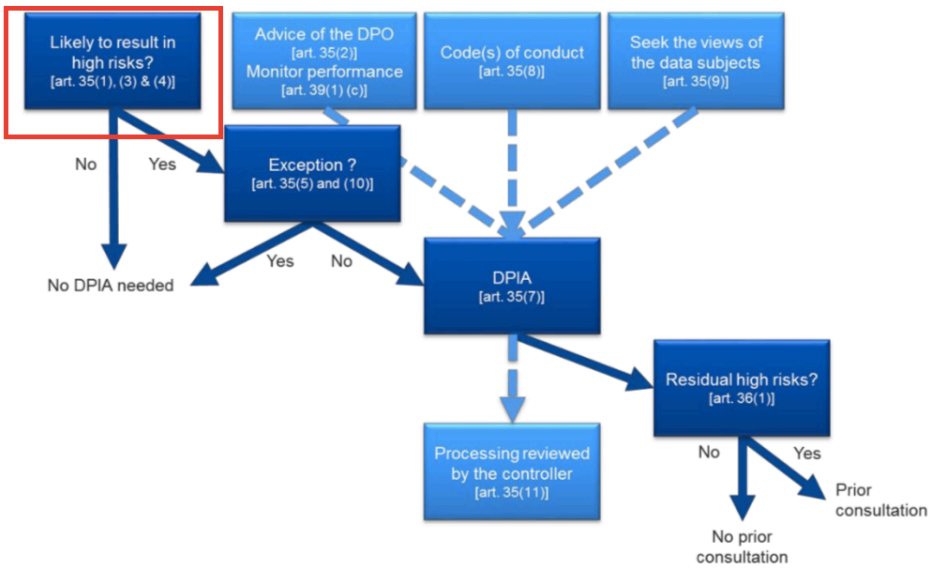
1.1.2.1.2 The pre-assessment leading to a DPIA

Where the pre-assessment concludes that the data processing operations enters into the scope of Article 35 or the criteria defined by the CNPD, data controllers shall conduct a DPIA on the data processing operation. In Luxembourg, considering the enlargement of the scope of application of Article 35 of the GDPR, data processing operations systematically fall under the requirements. Therefore, it appears less fastidious to systematically perform a DPIA than to complete first a pre-assessment, the conclusion of which leads to executing a DPIA.

1.1.2.1.3 One DPIA for a multiple data processings

Furthermore, GDPR specifies that data controllers may perform one DPIA covering multiple data processing operations. While GDPR introduces such a possibility to make multiple data processing operations more convenient to data controllers, it may in turn lead the data controllers to systematically conduct DPIAs without executing a pre-assessment on whether a DPIA is needed or not for the given operation.

The CNPD is actually furthering this application in its risk-based approach of GDPR. The reasoning is that, when carrying out a DPIA systematically, the focus of data controllers is less on assessing the need to carry out a DPIA, and more on the development of a coherent DPIA methodology.



SOURCE: WP29 GUIDELINES ON DPIA[12]

[12] WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of the GDPR, last revised and adopted on 4 October 2017

1.1.2.2 The performance of a DPIA

The GDPR provides a list of items that shall be considered when conducting the impact assessment. Therein it is emphasized that the DPIA shall in a first phase describe the context of the processing, in a second phase it shall analyse the controls guaranteeing the compliance with the proportionality and necessity principles and the protection of data subject's rights. In a third phase, the DPIA shall assess the risks associated with data security and demonstrate the safeguards and security measures to ensure the protection of personal data13. Lastly, the data controller, in view of the results of the previous phases, shall provide with mitigation measures and it shall validate the DPIA.

The GDPR does not provide with information regarding the form that the DPIA should take and the level of granularity of the information that shall be specified in the DPIA. Therefore, data controllers are required to develop their own DPIA methodology and to ensure that all the items indicated in article 35 (7) of the GDPR are covered by the demonstration. This absence of guidance from the regulation may result in laborious tasks for both the data controllers and the national authority.

Data controllers without exception shall conduct a DPIA on data processing operations, the development of a DPIA may however raise difficulties where the data controller has not designated a DPO, and where the person in charge of the data protection in the company does not have sufficient knowledge on data protection. There is therefore a risk that the DPIA developed and implemented by the data controller may not cover sufficiently the requirements of the GDPR or may lead the data controllers to assess the impacts wrongfully.

[13] Article 35 (7) of the GDPR

This constitutes also a significant risk towards the national authority as there is no guarantee that the impacts have rightfully been assessed and that they have been notified where they represent a high risk. In addition, as the GDPR does not specify the form that the DPIA should take, the national authority may receive DPIAs from data controllers that may take various forms such as Excel documents, Word documents, and of which the content, length and detail may vary significantly. As a consequence, to avert inconveniences, the French national authority, the *Commission Nationale de l'Informatique et des Libertés* (hereinafter the "CNIL"), has published a template of a DPIA that is made available in English language[14]. The data controllers may use and adjust it according to the specificity of their activities and it provides the data controllers with practical guidance as to the composition and structure it requires. On the other hand, the CNPD has not developed such a template DPIA but has published a document in which the items which the DPIA shall contain are specified[15].

Severity					
	Maximum	Medium	Medium	High	High
	Significant	Medium	Medium	High	High
	Limited	Low	Low	Medium	Medium
	Negligible	Low	Low	Medium	Medium
		Negligible	Limited	Significant	Maximum
		Likelihood			

EXAMPLE OF A DPIA RISK MATRIX / SOURCE: NO SOURCE, MADE FOR THE PURPOSE OF THIS PAPER

14 https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf
15 https://cnpd.public.lu/en/professionnels/obligations/AIPD.html

1.1.2.2.1 The consultation of the national authority

Where a data protection impact assessment indicates that the processing would result in a high risk without specific measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority.[16]

The GDPR conveys that the national authority shall be consulted if the risk assessed is qualified as "high" and where there is no mitigation measure, whereas the CNPD adopts a more lenient approach and requires to be consulted where the risk remains "high" after the implementation of mitigation measures[17]. In other words, according to the GDPR, the national authority's opinion is required based on the assessment on the inherent risk of the data processing, while according to the CNPD, the Luxembourgish authority shall be solicited based on the assessment on the residual risk of the data processing.

The CNPD requires to be consulted when the data controller has already determined mitigation measures, the authority then provides its opinion and recommendations not solely on the planned processing operation but also on the mitigation measures that the controller foresees to implement. The CNPD is therefore consulted to provide its opinion and recommendation solely for data processing operations presenting a significant risk that is not reduced by the implementation of measures. This may be interpreted as a way for the CNPD to be systematically informed of the highest risks that a company may present and to collaborate with the data controller from the early stage and to monitor the risks.

This may also be perceived as deterrent for the data controllers to implement such data processing operation that presents a high risk, considering that the CNPD will monitor this specific data processing operation.

16 Article 36 (1) of the GDPR

17 https://cnpd.public.lu/en/professionnels/obligations/AIPD.html

1.1.2.2.2 The DPIA to demonstrate accountability

Where data controllers conduct a DPIA on a data processing operation, they have to describe the processing activity and its risks for the data subject's rights. However, data controllers must also describe the measures that will be implemented in order to mitigate these risks. The DPIA shall therefore not be perceived by data controllers as a cumbersome exercise but as a way to demonstrate their accountability towards the national authority, as they present the measures that they intend to implement for reducing the risk and preventing the violation of the data subjects' rights. Subsequently, data controllers implement the measures that were identified in the DPIA in line with data privacy by design and by default in order to limit the potential impact of the data processing for the data subject and to mitigate the risk. The CNPD highlights that it is important to integrate the DPIA to the organisational process of the company and to ensure that the results of the DPIA influence the planning of the entity.

1.2 Section 2: The hybrid ex-ante and ex-post risk-based approach

1.2.1 Data privacy by design and by default

As expressed by the data protection officer interviewed (*See Appendix I)* from a data controller perspective, to demonstrate their compliance with the GDPR, data controllers shall evidence their accountability with regards to the data protection principles. Where, in a first phase, the data controllers have assessed the risk of a data processing operation that they intend to implement, naturally in a second phase the data controller shall determine and execute appropriate technical and organisational measures to protect the personal data that will be processed, to mitigate the risk and to ensure that solely the necessary data is processed[18]. Consequently, the application of the principle of data privacy by design and by default occurs in a second phase in the process of the data controllers to demonstrate their accountability. In order to substantiate their accountability, data controllers shall evidence the implementation of measures guaranteeing the respect of the data subject's rights. According to recital 90 of the GDPR the DPIA shall include measures, safeguards and mechanisms envisaged for mitigating the risk assessed. Therefore, in the course of the DPIA, the data controller assesses the technical and organisational measures that it should implement in order (i) to reduce the risks of the processing activity, and (ii) to limit the processing of personal data strictly to the data necessary for the conducting of its activities. As an example, in the DPIA template of the CNIL[19], in the section related to the risks data security risks, the data controllers shall describe for a given example of control (i) if the control is implemented or not; (ii) the data controllers shall then assess whether the control is sufficient for the data processing or if it can be improved on; (iii) lastly, the data controllers shall detail the corrective measures to improve the control. Further in the section related to the data minimisation of the DPIA template, the data controllers have to provide with a justification of the need for the data collection and its relevance to the data processing activity.

Where the data controllers could not provide a justification of the need to collect certain categories of personal data in the DPIA, the data controllers will design their systems to implement safeguards ensuring that this particular data is not collected and processed. The controls indicated in the DPIA and the related additional corrective actions for security improvements collectively constitute the measures that data controllers will design and integrate into their systems, in compliance with the article 25 of the GDPR to demonstrate their accountability.

[18] Article 25 of the GDPR

[19] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

1.2.2 The revision a posteriori of the technical and organisational measures

Article 25 of the GDPR states that the data controller shall implement appropriate technical and organisational measures both, at the time of the determination of the means for processing and at the time of the processing itself. Therefore, in order to implement such measures prior the beginning of the processing, data controllers shall assess the risks of the data processing and shall determine the measures at an early stage of the processing's development. This may entail a significant change for companies acting as data controllers, who have to adjust their project development processes in order to take into consideration the data privacy "by design and by default" in the conceptualisation of their projects.

Aside from the requirement of data controllers to implement appropriate technical and organisational measures at the time of the processing itself, GDPR also requires the data controllers to implement an *a posteriori* review of the measures during the course of the usage of the processing, in order to ensure that the measures remain appropriate to the data processing over the course of it life-cycle.

In light of the fact that a DPIA is reviewed when a change in the data processing risks occurs, this revision may therefore have an impact on the organisational and technical measures implemented by the data controllers to limit the risks of the data processing at the time of the DPIA. As a consequence, where the data controllers reconduct the impact assessment of a data processing, they shall as well reassess the measures implemented. The data controllers shall therefore assess the suitability of the measures within the context and purposes of processing, and adjust, in line of the characteristics of the data processing and the risks, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

However, article 25 does not specify any limitation with regards to the determination *a posteriori* of those measures to solely the time the DPIA is reassessed. The first paragraph of article 25 states that the technical and organisational measures shall be determined considering the "state of the art" and it is therefore understood that the data controllers shall implement measures that are current and advanced measured against the industry standard at the time. In order to ensure that the measures and systems enforced are advanced, the data controllers have to ensure a periodic reviews of them. Therefore, the data controller has to perform a frequent and systematic review of the measures and has to integrate such revision within the existing review processes. In practice, the function in charge of the risk management includes the revision of the abovementioned measures in the program of its periodic review. In fact, the difficulty that the risk manager encounters consists in the definition frequency and content of such reviews, an area where GDPR does not provide any further information

1.3 Section 3: The ex-post risk-based approach – conducting a severity assessment

1.3.1 The definition and identification of a personal data breach

1.3.1.1 The definition of a personal data breach

Outlined in article 33 of GDPR, in case of a personal data breach, the controller shall notify the personal data breach to the national authority not later than 72 hours after having become aware of it. In order to ensure the compliance with this requirement, the data controller shall develop a definition of what constitutes a data breach.

GDPR specifies that a personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"[20]. Furthermore, recital 85 of GDPR provides some specifications with regards to the damages that a personal data breach may cause for the data subjects; hence a personal data breach may result in physical, material or non-material damage such as loss of control over personal data, limitation of rights, but also discrimination, identity theft or fraud, loss of confidentiality of data protected by professional secrecy.

In fact, breaches can be of several types: (i) confidentiality breach, which consists of the unauthorised or accidental access or disclosure of personal data; (ii) availability breach, which consists of the unauthorized or accidental loss or destruction of personal data; (iii) and integrity breach which consists of the unauthorized or accidental modification of personal data. The personal data breach therefore shall be defined in terms of what kind of risk it represents for the data subject and what kind of damage it can cause.

The data controller shall define the personal data breach in accordance with the personal data it processes and considering its business requirements. For example, a data subject who opened a bank account in a bank and a data subject signing up for a grocery store membership card do not provide the same type of personal data and the damages a personal data breach may cause are significantly different. The data controllers in this example, the bank and the grocery store chain, are data controllers, both complete a data processing register and the DPIA to define the personal data breaches that may occur, albeit the content of these two documents will be vastly different.

[20] Article 4 (12) of the GDPR

The CNPD has conducted a study between May 2018 and September 2018 in order to establish what kind and how many personal data breaches occurred during this period[21]. The personal data breaches therein are classified in two categories: First, whether the breach was internal or external to the data controller and second, whether the data breach was malicious or non-malicious. Similarly, the definition done by data controllers should start at identifying what would constitute an internal and an external breach, and what can be considered a malicious and what a non-malicious breach.

Some data breaches are obvious, such as a computer hacks or a physical theft at the data controller's premises which is then an external and a malicious personal data breach. However, the difficulty for a data controller is to clearly define personal data breaches that are less evident. For example, where an employee sends an email with three of his co-workers in copy accidentally to the wrong client, agreeing to meet the client on a specific day, at a specific time, and specifying the wife of the client will be in attendance of the meeting, . It is not guaranteed that the employee reports the event to the person in charge of data protection in the company. The employee most probably will consider it as a non-event, even though in fact, the personal data of five persons was wrongly provided to an unrelated third person (the email addresses of the three co-workers, the name of the client and the name of his wife). In consequence, in order to avoid such grey zones, it is important that data controllers provide a definition of personal data breaches. This definition assists in preventing unidentified personal data breaches when they should have been identified; but it also eases the process to identify the type of breach.

1.3.1.2 The implementation of an identification process

After having defined what constitutes a personal data breach, the data controllers have to implement a process of personal data breach identification, which will eventually enable them to notify the breach to the national authority within the time limit of 72 hours, in compliance with article 33(1) of GDPR. The data controllers are not required to notify the personal data breach within 72 hours after the breach occurred, but rather the time-limit begins when the data controller has been made aware of the personal data breach, which can be materialized days or weeks after the actual breach event. However, the data controllers are required to demonstrate their accountability under GDPR principles, therefore they cannot justify that they did not notify the personal data breach to the national authority for the reason that they have not implemented sufficient processes and controls to detect such breach and hence did not become aware of it. In order to demonstrate their accountability, the data controllers have to implement a process to identify the personal data breach. The development of such process may vary depending on the size of the company and the type of personal data it processes, as outlined per example above.

[21] https://cnpd.public.lu/fr/actualites/national/2018/11/violation-donnees.html

In a practical application, for a small or medium-sized company (up to 250 employees), employees may be asked to simply send an email to the data protection officer or to the person in charge of data protection, with a given template containing some basic elements of the breach, such as the nature of the incident; the type of breach (internal or external, or both); the start / end date of the breach; the date of becoming aware of the breach; the categories (customer, employee,…) and number of people affected; type of data and number of records concerned; whether the breach is under control or not (with associated justification if not); the actions taken to close the breach; the actions identified to close the breach; potential consequences of the breach; the means of breach detection. For a big-sized company, in order to ease the process for the person in charge of data protection, it may be recommended for the company to create a platform where the employee specifies the personal data breach and where it is then categorised automatically depending on the information that the employee provides.

In any situation, where the data controllers have implemented such identification process, it needs to be ensured that employees will systematically report personal data breaches to the DPO or to the person in charge of the data protection in the company. The interviewed DPO (*Appendix I)* pointed out, that the most challenging topic for him as a DPO is change management. Even if the company specifies in its procedural framework and communicates to the employees the importance of such identification and the reports, it is not assured that the employees integrate and adopt it. Change management is not an easy process, even more so when the employees do not necessarily relate to the principle of personal data breach notification. It is therefore recommended to companies to train their employees regularly and raise their awareness on data protection, but also to not solely rely on its employees to detect data breaches, but develop electronic and manual controls.

1.3.1.3 Personal data breach as part of the security incident processes

The identification of a personal data breach should not only be seen as a stand-alone process that a company, acting as a data controller, has to implement. It is also part of the security incident process of a company as specified in recital 87 of GDPR. The personal data breach identification can be fully integrated into the already existing information security incident identification process and procedures. In practice, when the chief information security officer detects an incident and categorises it, he/she should have the possibility to specify that the incident that occurred may cause the breach of personal data; as a result, the person in charge of the data protection will be made aware of such incident. This specification of recital 87 provides the data controllers with indication that the requirements laid down in GDPR are not contrasting with the controls that the data controllers already performed, they can be embedded in the existing processes. However, a distinction shall be made between a usual security incident and a personal data breach, the difference resides in the severity assessment that is conducted on the incident.

1.3.2 The assessment of the severity

1.3.2.1 The necessity to develop a methodology

In the words of article 33 of GDPR, the data controllers are required to notify to the national authority of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. In addition, it is further specified that the data controller shall communicate the personal data breach to the data subject where the personal data breach is likely to result in a high risk to rights and freedoms of natural persons[22]. Accordingly, the data controllers are required to implement a methodology to assess the severity of the personal data breach and to act upon the results. GDPR does not provide the data controllers with further guidance on how the severity assessment shall be conducted, data controllers are required to develop their own breach severity assessment. In practical experience, the definition of the breach severity assessment methodology is usually similar to the security incident assessment that has been previously defined and implemented. While the security incident assessment addresses the severity of the incident for the company, the breach severity assessment addresses the risk of the breach for the data subject's rights. The spirit behind GDPR is to ensure a better protection of the data subject's personal data, therefore the assessment of the risk in case of a breach cannot be conducted in the same manner as the security incident assessment. The former relates to risks posed toward data subjects and their personal data, while the latter addressed risks threatening the company itself. For this reason, data controllers have to define methodologies distinct from the security incident assessment. The European Union Agency for Network and Information Security (also called the "ENISA") has published in December 2013, before publication of GDPR, an exhaustive methodology to conduct a personal data severity breach assessment[23]. According to the methodology, the personal data breach is assessed by assessing individually three aspects of the personal data breach, (i) the data processing context, (ii) the ease of identification which assesses how easy it would be for a third party to identify the data subject's if he accesses to the personal data that was breached, and (iii) the circumstances of the breach. Thereafter, the three aspects are individually scored and then added to a formula which calculates the overall severity. The calculated result of the overall severity is thereafter analysed according to a scoring matrix.

[22] Article 34(1) of the GDPR

[23] https://www.enisa.europa.eu/publications/dbn-severity

1.3.2.2 The choice of methodology

Since GDPR does not provide the data controllers with a methodology to assess the severity of the personal data breach, the data controllers have the free choice to decide to develop their own methodology or to adopt a methodology that is inspired from the methodology of ENISA. The adoption of the ENISA methodology by data controllers may be of great benefit for a company as the methodology is highly detailed. The methodology developed by ENISA offers a high level of granularity and practical examples that it does not leave any place for subjectivity and ensures the severity of the personal data breach is assessed objectively.

The objectivity in the severity assessment is essential for a data controller as it provides guarantee that the assessment is performed with consistency, and the severity score is consistent with the characteristics of the breach. Where data controllers resolve to develop and implement their own severity assessment methodology, the task may easily become ponderous. In addition, there is a risk for data controllers that the methodology is not sufficiently detailed to cover the principles of GDPR and to establish the correct score of the personal data breach, elements necessary to demonstrate the accountability of the data controllers. The governance decision to be taken shall be based on the capabilities of the data controller to develop its own methodology but also on the volume of personal data breaches he or she may encounter. As mentioned above, data controllers have only 72 hours to assess the severity of the breach and to notify it to the national authority. Therefore, the methodology that they decide to implement has to be accessible, easy to use and accurate, in order to enable them to assess the severity of the breach without any unnecessary delay.

Reporting decision	Severity value from the scoring matrix	Severity level	Impact on data subjects
Reporting to the national authority	<2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)
Reporting to the national authority	2≤x<3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.)
Reporting to the national authority and to the data subject	3≤x<4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.)
Reporting to the national authority and to the data subject	4≤SE	Very high	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long term psychological or physical ailments, death, etc)

Example of overall severity impact assessment inspired from the ENISA methodology / Source: No source, made for the purpose of this paper

1.3.3 The decision to notify the breach

1.3.3.1 The notification to the national authority

Regardless of the methodology used by the data controller to assess the severity of the personal data breach, where the result of the assessment is that the personal data breach presents a risk for the data subject's rights, the data controller shall notify the breach to the national authority. In line with the risk-based approach of GDPR, even where the risk presented is low, the Information Commissioners Office, the national data protection authority of the United Kingdom (hereinafter the "ICO"), specifies that if it is likely that there is a risk for the data subject's rights then the data controllers shall notify him or her[24]. Therefore, national authorities across the European Union apply a stricter approach than the GDPR provides.

The implementation of a substantial process to identify the personal data breach, as discussed previously, is a significant base for the data controllers to collect the necessary information that shall be provided to the national authority for the notification. Where the individual identifying the personal data breach provides the necessary details and granularity with regards to the nature of the breach, the consequences of the breach and the measures taken to address the breach, the person in charge of the data protection or the DPO has all the necessary information to notify the national authority without undue delay.

1.3.3.2 The communication to the data subject

While the notification of the personal data breach to the national authority is automatic when the breach presents a risk for the data subject's rights, the communication to the data subject is not automatic and appears to be less in line with the risk-based approach of GDPR. According to GDPR, the data controllers shall communicate the incident to the data subject solely when the breach presents a high risk for him/her. The consequences of this restriction is that the data subject will not be informed where his/her personal data may have been the object of a breach and where his personal data may be diffused and/or misused, due to the results of the performed risk assessment. However, in article 34, GDPR specifies that the national authority may decide to qualify the personal breach as reportable to the data subject due to the likelihood and the severity of the breach. In addition, data controllers may take the decision to communicate the personal data breach to the data subjects also when the breach presents a lesser risk than high (i.e. low and medium). This is a business decision that the data controllers may take in order to guarantee a greater transparency with clients as to the protection of their data.

[24]https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

The provisions of GDPR raise the awareness of controllers which data they have at risk and to what extent. The data controllers are required to assess the risk of the data processing ex-ante, but also to design their IT systems and data processing around the thought that it shall reduce the risks posed to personal data and assess the severity of the personal data breach. GDPR indisputably provides with what can be characterised as a risk-based approach of data protection; however, besides the great philosophy behind its provisions, GDPR fails to provide the data controllers with sufficient practical guidance to enable them to transform the theoretical principles of the data protection into practicality.

As a consequence, several European national authorities such as the UK ICO and the French CNIL, or the ENISA assist the European Data Protection Board (hereafter the "EDPB") in the provision of practical guidance and opinions aiming at accompanying the professionals in their implementation of GDPR. However, while such guidelines ease the process of implementation, they do not provide tailored support to particular challenges in any specific industry. One crucial challenge especially Luxembourg based data controllers face is the recording of their data processing activities as required by article 30 of GDPR. In order to assist the controllers in establishing a record of processing activities under their responsibility, the CNIL has provided a model of data registry that may be enforced as such[25]. As a consequence, the difficulty of the data controllers resides less in the formatting of the registry of data processing activities, and more in conducting an extensive work of research and mapping internally, to identify all the data processing that are already implemented in the company prior to GDPR and to define the characteristics of the new data processing activities to be implemented post GDPR go-live. This task of research and mapping raises significant difficulties for Luxembourg based data controllers within the financial industry, as Luxembourg's most important industry carries some of the most valuable personal data

[25]https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

2 Chapter 2: An insight on practical challenges encountered by the Luxembourg based data controllers for the implementation of GDPR

2.1 Section 1: The crucial determination of " lawfulness of processing"

2.1.1 The consequences of a lawful basis wrongfully defined

2.1.1.1 The right to retain personal data based on a legal obligation or the public interest

In the terms of article 5 (1)(b) of GDPR, personal data shall be collected for "specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". In order to demonstrate its accountability with article 5, data controllers shall determine the lawfulness of the processing on which it bases the data processing activity. GDPR specifies that a data processing activity is qualified as lawful where "(i) it is based on the given consent of the data subject, (ii) the processing is necessary to carry out a contract in which the data subject is a party, (iii) the processing is necessary for the compliance with legal obligations, (iv) in order to protect the vital interests of the data subjects, (v) for the legitimate interest of the data controller or (vi) for the performance of tasks carried out in the public interest"[26]. Accordingly, the data controllers shall identify the lawful basis for each data processing activity and shall specify it in the data registry they have implemented. Depending on the lawful basis that is specified, the obligations of the data controllers towards the processing of the data may vary significantly. GDPR specifies that the data subject's rights are limited where the data processing is necessary for the compliance with a legal obligation or for the performance of a task carried out in the public interest[27].

Therefore, for example the right to erasure, one of the key rights data subjects have under GDPR, does not apply where the data processing is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest[28].In contrast, where the data processing is based on the consent of the data subject or on contractual obligations, the data subject may request to exercise his or her right to erasure at any point in time. As a consequence, where data controllers identify the lawful basis for a data processing, they shall ensure to select the appropriate lawful basis, not as to reduce the rights of the data subjects but as to ensure that they do not erase upon request data that there are legally required to keep. As a practical example, an employee resigning from his position at a company located in Luxembourg and requests his former employer to erase all his personal data, including the personal data on his working contract that ceases to exist.

[26] Article 6 of the GDPR

[27] Articles 17(3), 18(2), 20(3), 21(6) of the GDPR

[28] Article 17 (3) of the GDPR

Where the employer has documented a data registry including the information related to the lawful basis for the processing personal data, the employer notices that the processing of the working contract of its employees is based on a legal obligation and that the retention period is ten years after the end of the contractual relationship[29]. Consequently, he cannot satisfy the request of the employee as has to inform him accordingly.

2.1.1.2 The requirement of the national authority's authorisation

As a result of the DPIA (*see Chapter 1 Section 1*), where the data processing presents a high risk towards the rights of the data subjects, data controllers are required to consult the national authority (*see Chapter 1 Section 1*). Furthermore, GDPR specifies that where the processing is related to a task carried out by the controller in the public interest, the data controllers shall obtain the prior authorisation from the national authority, regardless of the risk it presents for the rights of the data subject. Depending on which lawful basis data controllers identify for a processing activity, they are not only required to notify the national authority prior the conduct of such processing, but are to obtain the active authorisation of the national authority, which can be time consuming and burdensome. Subsequently, where the data controllers have not identified the correct lawful basis, where applicable, they are inadvertently not in compliance with the obligation to obtain prior authorisation of the national authority or in the contrary (albeit less serious) they may request the authorisation of the national authority where this not warranted.

2.1.1.3 The consent as a tool for the transfer to a non-adequate country

As the financial industry is a highly regulated sector with the application of, amongst others, the Financial Regulations and together with regulations related to anti-money laundering, a significant amount of personal data is required to be collected and processed based on those regulations. Therefore, data controllers in Luxembourg acting in the financial industry do not base the processing of personal data on the data subject's consent but on legal obligations or on public interest (in the case of AML). However, in the terms of GDPR, in the absence of appropriate safeguards or binding corporate rules, where data controllers would like to transfer personal data to a third country in cases with no reason related to public interest, data controllers may base this transfer on the consent of the data subject[30]. As a consequence, data controllers may decide to request the consent of the data subject to conduct such transfer even for data related where the grounds for collecting it are based on legal requirements.

[29] Article 16 of the Luxembourgish trade code

[30] Article 49(1) of the GDPR

While obtaining the consent of the data subject may be an advantage in such situations, it presents some constrains as to the conditions required for the consent to be valid and this poses a risk for the data controller, as the consent can be withdrawn at any moment or not granted in the beginning. Accordingly, the consent of the data subject shall be free, explicit, informed and unambiguous[31] which requires a certain effort of implementation for the data controllers to ensure that the collected consent complies with those requirements. In addition, as the consent of the data subject can be withdrawn at any moment, this may raise some uncertainty for the business processes of the data controllers and their activities. Where the data subject withdraws his/her consent, the data controller either (i) has to define another legal basis for the transfer of data, or (ii) has to stop the processing of the personal data.

Subsequently, it is essential for the data controllers to correctly identify the appropriate lawful basis for each data processing in order to avoid any unnecessary constraints and to avoid any doubt and uncertainty as to the rights he or she has over the collected personal data and equally have a clear view on the resulting obligations.

2.1.2 The current conflict of lawful basis in theory and in practice

2.1.2.1 The problems posed by the recent anti-money laundering law in Luxembourg

As outlined above, it may appear laborious for a Luxembourg based data controllers to identify – for each data processing – the accurate and least-restricting lawful basis. Another difficulty for the data controllers is to ensure that the lawful basis for the data collection remains valid during the data lifecycle.

As outlined in the Luxembourgish law of 13 February 2018[32] (hereafter the "AML Law") implementing the provisions of the European Directive 2018/843[33] (hereafter "AML IV") with regards to preventing anti-money laundering and terrorist financing, a question may be raised as to the lawful basis for the processing of personal data related to anti-money laundering.
AML IV states that the processing of personal data in the context of this directive shall be considered to be a matter of public interest. The AML Law further specifies that "Personal data shall be processed on the basis of this Law by professionals only for the purpose of the prevention of money laundering and terrorist financing and shall not be further processed in a manner incompatible with the said purposes. The processing of personal data on the basis of this law for any other purpose is prohibited"[34]

[31] Article 4 (11) of the GDPR

[32] http://legilux.public.lu/eli/etat/leg/loi/2018/02/13/a131/jo

[33] Directive 2018/843 amending the Directive 2015/849

[34] Article 6(10) (the original text is only available in French language, provided is a free translation).

The personal data processed in this context may be any type of personal data that enables the data controllers to have sufficient information to assess the potential risks the data subjects present in terms of anti-money laundering and financing of terrorism. In Luxembourg established practice every stakeholder of the financial industry, whether it is a bank, an investment firm, an asset manager etc., conducts AML/CTF (Counter terrorism financing) assessments. For this purpose, the data controllers collect a considerable amount of information, either directly from the data subject or from external sources, on the data subject's financial situation, the origin of his or her funds, the use of the funds, information as regards to the family and relations, amongst others.

According to the AML IV and the AML Law, data controllers may collect and process personal data for the purpose of the public interest and therefore define the lawful basis for such processes accordingly. However, the AML Law specifies that "the processing of personal data on the basis of this law for any other purpose is prohibited*"*. This provision raises significant questions as it means that personal data collected on the basis of prevention of money laundering can be processed for other purposes is generally allowed, but it will not be based on the public interest justification provided by the AML Law.

In practice, it means that personal data collected on the basis of public interest, may be processed in such a way that it does not comply with lawful basis of public interest. The data controllers will perform the AML/CTF controls based on the public interest, however the further processing of the personal data collected in this context is not considered as based on the lawful basis of public interest. The thin line of differentiation resides in the fact that the collection of personal data forms one data processing, and the use of the personal data collected, by, for example, providing it to different stakeholders of the bank that are not implied in the AML/CTF process, forms a different data processing. The latter cannot be based on the lawful basis of public interest. As an example, a banker collecting information about his client for the AML/CTF purposes bases his process on the public interest, however when he provides the information collected to his client-onboarding colleague to record the information in the client database which is not related to the AML/CTF the second process requires a new justification. The CNPD has not yet expressed any guidance in this regard, but it constitutes undoubtedly a challenge for the Luxembourg- data controllers that need to ensure the accurate determination of the lawful basis for each usage they make of the personal data they collect and at the same time efficiently service clients and not request the same piece of information at multiple points in time. Where the legal basis for data processing appears to be obvious when it results from a contractual or a legal obligation, the definition of the legal basis for other personal data processing may be less evident and more cumbersome for the data controllers; and the task may easily become arduous considering that the result of such assessment may limit the possibilities of the data controllers to process the data or may require them to comply with additional obligations to ensure their compliance with the regulation.

At the same time, customers are increasingly demanding with regards to the service offered to them and should be serviced, for commercial as well as cost reasons, as efficiently as possible.

2.1.2.2 The conflict related to the MiFID II provisions

The delegated regulation 2017/565 supplementing MiFID II (hereafter referred to as "MiFIR") and the MiFID II itself specify that investment firms shall implement and maintain an effective recording of telephone conversations and electronic communications policy relating to, amongst others, the provision of services that relate to the reception, transmission and execution of client orders.[35] An investment firm for this purpose is any legal person whose regular occupation or business is the provision of one or more investment services to third parties and/or the performance of one or more investment activities on a professional basis. As a consequence, since the entering into force of MiFID II on 3 January 2018, any company qualifying as an investment firm is required to record all telephone conversations and electronic communications related to a transaction. Therefore, the investment firm acting as a data controller collects and processes this personal data based on the lawful basis of the legal obligation. In practice this requirement of MiFID II raises challenges regarding the lawful basis for the personal data that is included in a telephone conversation or in an email if information is included that does not strictly related to orders or transactions. A client calling his banker in order to purchase for fifty shares of the company Apple Inc. will be recorded based on the legal obligations of MiFID II. However, during the same conversation, the client tells his banker about his private life and his wife. This information about the client's wife is part of the conversation that is recorded and the question that may be raised is on which lawful basis this personal data is processed. For the sake of the relationship with the client, the banker cannot prevent his client to tell any personal information that is not related to the transaction during the recorded communication. This may be a demanding question to solve for data controller, as it would require them to delete parts of the phone conversation for the reason that it does not enter into the scope of the MiFID II and that there is no lawful basis for the processing of this particular data. This is, aside from many challenges, a major technical hurdle.

[35] Article 76 of MiFIR and article 16(7) of MiFID II

2.2 Section 2: The complex inventory of the personal data processing

2.2.1 The complexity of information flows

GDPR states that each data controller shall maintain a record of the processing activities[36]. Personal data processing in this meaning is any operation or set of operations which is performed on personal data or on sets of personal data, regardless if such processes are automated or not. Examples are collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[37]. In other words, any action either passive (such as receiving personal data) or active (such as sending personal data, storing it, erasing it) performed on personal data is considered to be a personal data processing activity.

In addition, the registry shall cover all the processing operations of the data controllers in such a way as to enable the national authority to use it for monitoring of those processing operations[38]. Therefore, data controllers are required to map exhaustively all their personal data processing activities; an exercise whose difficulty increases exponentially with the depth and extent of the company specific information flows. With regards to the completeness of the data processing registry, data controllers face questions with regards to the granularity expected by national authorities. By way of example, a bank acting as data controller may indicate as one of the processing activity "the management of bank accounts". Another bank in the same position may define the activities as "the management of real estate assets in the context of the management of accounts". The CNPD has not provided yet any guidance to data controllers based in Luxembourg what their expectations is and therefore data controllers have to make a business risk decision and to define the level of granularity their data registry shall demonstrate and what level of granularity can be maintained over the course of the business. The above banking example represents an example of a data processor with significant amounts of personal data at its disposal. If one considers only one aspects of the activities of such a bank, i.e. providing retail banking services to clients, the bank still performs a substantial number of personal data processing for only one of the many services it offers. A number that multiplies with every service line or service offering the bank has on its shelf.

[36] Article 30 of the GDPR

[37] Article 4 of the GDPR

[38] Article 82 of the GDPR

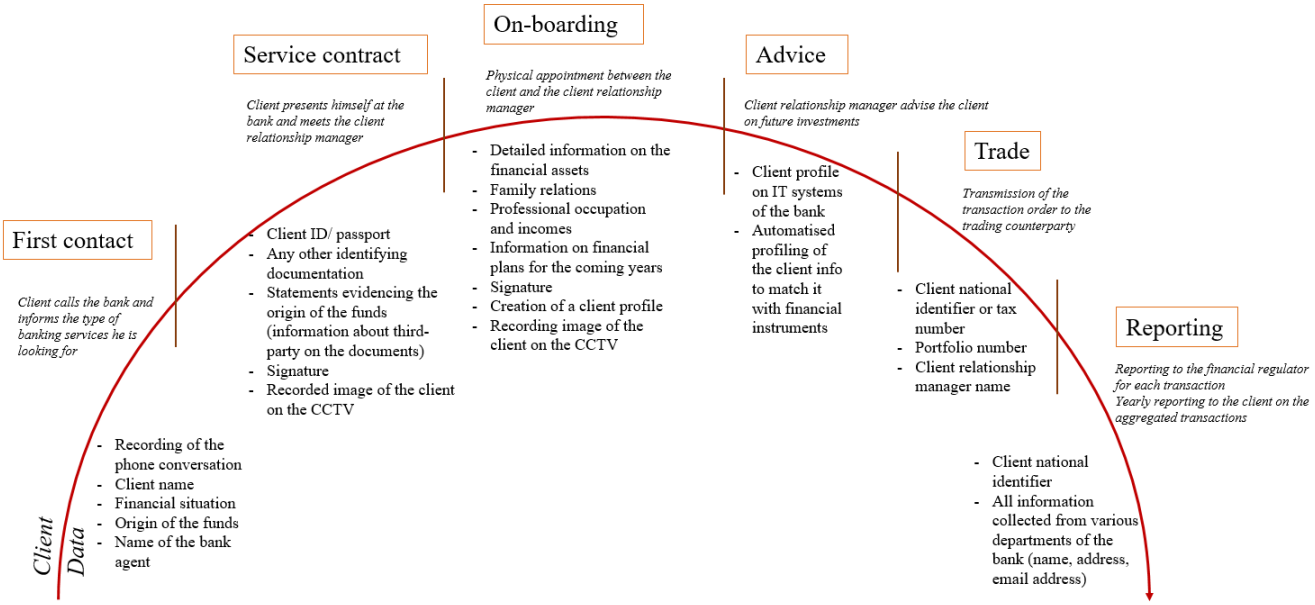
If looked at closely, even during the onset of the relationship between the bank and its client at least eight personal data processing activities can be identified for the sole purpose of opening a bank account:

- The client relationship manager of the bank (hereafter the "CRM") collects personal information about his or her client on paper format (1) and then adds the information into the client relationship IT system (2).
- The personal data added into the system is provided to the data warehouse (for future processing) (3) and to the data lake (for analytics and big-data assessments) set up by the bank (4);
- Assuming the IT systems of the bank are not connected to each other, the personal data from the client relationship IT system are collected by another employee (5) and transposed to the IT system used to perform banking transactions (6);
- Afterward, the personal data is used to create an online profile and a web-banking access for the client (7);
- Finally, a bank is subject to strict "disaster recovery" requirements. Therefore, the personal data is replicated in the back-up process of the bank (8).

This exercise of deconstruction and analysis of each activity of a bank (by way of example), shall not be solely conducted on activities that are known for processing personal data, but it shall be conducted on all activities of data controllers in order to ensure that personal data processing activities are identified, even in processes that seem on the out-set unlikely to involve such processes. The initial task is therefore a horrendous effort requiring dedicated teams with considerable time outside of their day-to-day activities.

The challenge is further illustrated by looking at a very simple client relationship life-cycle extract of investment services (i.e. investment advice). In addition to the above outlined assessment, below represents a mere illustration of contact points and the usual data exchanges at these points. This does not yet extent the assessment to the systems a bank might use to support these tasks:

The provision of investment services to a natural person



SOURCE: NO SOURCE, MADE FOR THE PURPOSE OF THIS PAPER BASED ON MIFID II CLIENT ADVISOR TRAINING MATERIALS

Still, the examples provided represent only a narrowed portion of the personal data processing activities that data controllers conduct in their everyday business activities. Even in the example of the banking relationship, the aspects that are mentioned above cover only the activities of the bank towards its clients. However, the private bank acting as a data controller conducts personal data processing activities in the context of several other business duties, i.e. processing the personal data of its employees or personal data processing related to service providers. Aside from processing data for its own purposes, the data processor also transfers personal data to external parties such as a regulators or other group entities.

2.2.2 The complexity identification of the personal data

Article 30(1)(c) of GDPR specifies that the data processing registry shall provide a description of categories of personal data. For each personal data processing activity, the data controllers shall specify the categories of personal data concerned. This exercise may present challenges for the data controllers considering that some personal data is not always easy to classify .

A CRM from a bank has an appointment with a client writes a brief report to summarise the discussion he or she had with the client. The report is written in a defined template within the client relationship software which foresees information related to the current financial situation of the client and the investments he foresees to perform as outcome of the meeting. These fields are hard-coded and reserved for their purposes. However, some fields are free of label and can be used as “Miscellaneous” or “Comments”, and the CRM may specify any kind of information therein that he may considered as relevant.

For example, the CRM may specify in such field that the client's wife has a non-curable disease, as he considers that this information may have consequences on the financial situation of his client and the future life-cycle of his portfolio. However, the information provided is sensitive data about a third-party data subject, specified in the IT system of the bank, which constitutes a personal data processing. As a consequence, the bank processes sensitive data of a data subject without necessarily being aware of it nor is the data subject, in this case a third party, aware of such processing.

Data controllers encounter difficulties to conduct the inventory of their data processing activities and the related personal data due to the variety of personal data they process, ranging from signatures, to email addresses or non-static information, provided in the context of a meeting. The difficulties increase by unforeseen data that may be essential for a relationship, but cannot be accounted for by categories or templates (i.e. a change of family situation affecting wealth).

Considering the above outlined difficulties, the importance for data controllers to implement data privacy measures by design and by default are essential, not only to mitigate risks for the data subjects, but also to gain control and transparency on the data processing activities they conduct and the personal data they process.

2.3 Section 3: The challenges faced by different types of processors

The tasks of data controllers laid out within GDPR are uniform for all data controllers, regardless of industry, size or type of operations. This includes, as above outlined, the maintenance of a data processing registry and the need to conduct a gap analysis of the personal data they process in order to ensure that the personal data is proportionate, secured, current, not stored longer than necessary and that each personal data processing activity is based on a lawful basis. Simultaneously, the data controllers shall implement process and procedures that enable them to satisfy to the requests of the data subjects to exercise their rights[39] and to identify and notify the risks of the personal data processing regardless of how cumbersome this may be in specific types of industries. However, while the requirements posed towards data controllers are the same, the challenges encountered while implementing GDPR vary significantly. This is best illustrated by analysing two different examples of stakeholders of the financial sector in Luxembourg, both are investment firms, however the first one is a company conducting several activities while the second one is a company having a single activity.

[39] Articles 15, 16, 17, 18, 20 of the GDPR

An investment firm having several activities may provide services to different types of clients such as retail client (*ex: individuals, small companies*), institutional client (*ex: pension funds, infrastructure providers*), corporate clients (ex: *investment banks*) and peers or counterparties (*ex: other investment firms*). In addition, the investment firm may have its own trading room, and may also be active in philanthropy, fundraising all while employing hundreds of employees.

The second example is a company pursuing a single activity such as private banking to high-net-worth clients and employs one hundred employees.

Albeit facing the same set of rules, the investment firm offering several services to various client types encounters significantly more e difficulties than the single-service investment firm with regards to the identification of data processing activities and personal data, since the former is required to identify the personal data processing for each activity it offers. However, an investment firm having one activity may face extensive difficulties with regards to the change management. In fact, the DPO or the person in charge of data protection encounters more difficulties to implement changes in a small investment firm than his or her counterpart in a big-size investment firm where processes and procedures are systematically implemented and controlled. In this regard, an investment firm with a single activity does not have the organisational structure to support the implementation of the GDPR and to perform the related controls. Thus, it may be difficult for these investment firms to require its compliance function, acting alone, to develop the sufficient knowledge and experience to develop appropriate procedures and controls with regards to the data protection and implement them thoroughly in the organisation. This is not yet considering, that the same officer has to fulfil all his other legal and change management tasks that the industry faces.

Finally, GDPR applies to companies regardless of their size, nature or industry, as outlined above. While the financial industry in the past years has been used to change management and has at least once revamped the overall compliance framework and therefore is familiar with its ins and outs, other industries have not been subject to such a flood of change. A sizeable manufacturing firm in rural Luxembourg, for example, will face the very first challenge in adopting a change management culture and integrate such “distraction” into its day-to-day tasks.

3 Conclusion

The stakeholders of the financial industry in Luxembourg are accustomed to the compliance process associated with European regulations and directives. In fact, the latest European directive that entered into force on 3 January 2018[40] took investment firms in average three to four years of implementation work. Therefore, considering that prior to GDPR, the data protection in Luxembourg was already well advanced, the entering into force of GDPR and the subsequent Luxembourgish law of 1 August 2018[41], was simply perceived as an additional regulation to implement for the financial industry. GDPR does not re-build data protection in Luxembourg as such, since the largest portion of stakeholders (being those of the financial industry) generally cherish professional secrecy and execute all necessary safeguards to guarantee the protection of the personal data of their clients – albeit driven more out of the hay-days of banking secrecy rather than the careful protection of personal data rights. However, GDPR requires to prepare new documentation with regards to personal data processing activities and the associated risks and to introduce new or strengthen certain controls. Those two aspects nevertheless create challenges for the financial industry in Luxembourg due to the limited provision of practical guidance (*see Chapter 1*).

Within European legislation, one of the two key acts are either directives or regulations. The former leaving room for implementation of member states, the latter strictly providing rules and laws that cannot be altered on national level. Where the absence of details within a European directive is expected and is balanced by the provision of guidelines issued by European authorities, the absence of practical guidance in the European regulation is unexpected and, together with the lack of a strong regulator presence, creates major uncertainties for data controllers. Therefore, Luxembourgish data controllers seek for guidance in the publications of neighbouring national authorities, like the ICO and the CNIL, and work together with the CNPD in order to develop the best practices. The role of the CNPD in Luxembourg is essential not solely as a national authority but to accompany the data controllers in the development of their documentation and their processes. In this sense Luxembourg is unique, as the regulator might lack strong opinions and guidance, however is actively collaborating and generally allows guidance to be taken from countries other than Luxembourg.

[40] The MiFID II

[41] Luxembourgish law implementing the GDPR's requirements
http://data.legilux.public.lu/file/eli-etat-leg-loi-2018-08-01-a686-jo-fr-pdf.pdf

At the end of the summer 2018, the CNPD has selected a few market stakeholders in order to plan a visit on-site at their premises. The CNPD has requested from the selected companies to provide basic information as to their readiness with GDPR. This was not to criticize or punish the selected market stakeholders but rather to develop guidance and assistance directly in conjunction with the industry. The CNPD thereby does not adapt a punitive approach towards the Luxembourgish industry, but rather accompanies stakeholders and provides them with recommendations. The data controllers in Luxembourg benefit from these recommendations to implement practices that enable them to be compliant with the requirements of GDPR but also to develop practices that are not too restrictive which allow for agility within the processing of personal data.

Data controllers perceive GDPR most commonly as a business constraint, due to the tremendous amount of work it requires to identify and categorise the personal data processing activities, not only initially but also ongoing. However, GDPR, when correctly implemented, does not limit the activities of the data controllers. For instance, data controllers may transfer personal data according to their needs without any restrictions[42], subject to adequate implementation of the framework of GDPR. GDPR is a regulation that was necessary to provide a regulatory framework adapted to the digital and technological world of 2018, reaching – much like the information it regulates – across state boundaries. When implemented correctly, GDPR offers to gain the upper hand in a world that is dictated and driven by information, even if that information passes through systems that date back a decade or more. Finally, the framework provided by GDPR is the inevitable regulatory basis for much of the next decade of systems and information. Be that blockchain integrations or be that open architecture driven by technological and financial start-ups, benefitting from the European directive on payment services[43] that enables third party payment providers to request access to information on payments and bank accounts of clients. GDPR helps us to guard one of our biggest assets in the digital age – our personal information.

[42] Recital 101 of the GDPR

[43] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=FR

4 Appendix 1: The interview of the DPO of an international large company

The DPO of an international large company providing professional services in Luxembourg (hereafter "the Company") kindly accepted to answer to some questions as regards to his activities of DPO and the implementation of the GDPR in his firm[44]. The Company employs 3000 people in Luxembourg and provides services such as audit, tax and advisory to clients that can vary from local and middle market entrepreneurs to large multinational companies located in Luxembourg and the enclosing area. The Company is part of the worldwide network of in 160 countries. The DPO of the Company is in charge of the implementation of the GDPR in the company and of ensuring the compliance of the Company with the European and Luxembourgish regulatory framework with also considering the specificities of the Luxembourgish market and the financial industry.

The hereunder questions were asked to the DPO during an interview that was conducted in French language in the sole context of the present thesis, the answers to the questions provide an insight on the practical challenges that the GDPR may arise; but the Company and its DPO cannot be held liable of the answers provided.

4.1 GDPR readiness

4.1.1 How does the DPO prepares for a potential visit of the CNPD?

Under the amended Law of 2002[45], the CNPD may order the company to provide it with any information it requires for the performance of its duties. The CNPD may therefore conduct investigation in the form of data protection audits and to access to all premises of the company and any means of processing, referred as to "a visit".

According to the DPO of the Company preparedness for a potential visit of the CNPD hinges on the development of the compliance of the company to the GDPR. Depending on the vision and the strategy of the company the means to ensure the compliance with the GDPR may vary, however to define the strategy of the company, it may imply for several stakeholders to work together, those stakeholders may be the DPO, the data management officer, the compliance department and the risk management department. Whether the CNPD would request to receive some documentation by email or would conduct an audit on-site, the company should

[44] In order to guarantee for the Company to not be held liable for this paper; and in order to ensure that the answers provided cannot be use as advice; and to keep the anonymity of the LL.M. candidate working for this firm, the name of the Company is not revealed.

45 http://legilux.public.lu/eli/etat/leg/loi/2002/08/02/n2/jo

demonstrate that it complies with the principle of accountability, the company may then define a general data protection policy and then establish a procedural framework.

4.1.2 The Company is a part of a worldwide network, including firms (having the same brand name) located across the world, are you aligned with them on your approach of the GDPR? Or is any firm developing its own methodologies to approach the GDPR?

The Company is not a branch company and is therefore not a sister company of the other offices having the same brand name across the world. However, The Company is part of the global network and the different firms may collaborate and work together.

According to the DPO of the Company, in the context of the exchange of information between the other offices that are located not solely in the EU but also across the world in countries that may not have implemented adequate measures, the global network works together to establish common standards for the exchange of data. In line with the risk-based approach of the GDPR, the firms implement measures to gain some comfort in the exchange of data. Therefore, each of the firms adopts its own policies, but similarly for the exchange of information with any other company, the firms implement a framework to regulate the exchange of data with for example the integration of binding corporate rules. However, they are working together to develop best practices.

4.1.3 Will the Company apply for a certification as mentioned in the article 42 of the GDPR? And why?

The Company complies with the standards of the ISO/IEC 27001 and ISO/IEC 27002 certifications for keeping information assets secure[46].

The Company is considering applying for a certification as mentioned in the article 42 of the GDPR for the reason that the certification is provided by an external body confirming that the Company complies with its accountability duties as defined in the GDPR. The certification may also be considered as a mean to receive guidance on developments areas to ensure full compliance with the regulation.

46 https://www.iso.org/isoiec-27001-information-security.html

4.1.4 How did the DPO build his knowledge on the GDPR?

The current DPO of the Company has a legal background and is qualified lawyer. However, his knowledge of the GDPR is empirical and he developed it through his experiences.

4.1.5 How is the team of the DPO composed of?

The DPO of the Company is working together with a team currently composed of a data protection analyst for IT security, a business and jurist analyst and a project manager. The DPO and his team work together with other teams of the Company such as the compliance department, the legal department and IT department.

4.1.6 Has the DPO received questions from the employees or clients of the Company with regards to the exercise of their rights?

Since the entering into force of the GDPR, it has become easy to request access to your own personal data, websites were developed to ease the process such as mydatarequest.com, the process has become remarkably easy and data subjects are requested to access to their data from all the companies they have been in contact with. The data subjects of the Company are the clients of the company and also the 3000 employees, contractual parties.

According to the DPO of the Company, since 25 May 2018, several data subjects requested to exercise their rights and more particularly the right to erasure. It is born in mind that the company complies with its regulatory obligations to the extent where the personal data of the data subject cannot be erased where the company needs to have such data to comply with its legal obligations.

4.1.7 How does the DPO perceive the CNPD? Would you say the authority is working together with the industry or is having a punitive approach?

On 28 September 2018, the CNPD has published a feedback on the data breaches that were notified since 25 May 2018. This action of the CNPD is to raise awareness of the data controllers and the data processors in view of transparency[47].

In his opinion, the DPO of the Company considers that the CNPD is working together with the companies located in Luxembourg in a constructive way. The CNPD takes the responsibility to increase awareness and to educate the companies instead of adopting a punitive program.

47 https://cnpd.public.lu/fr/actualites/national/2018/11/violation-donnees.html

4.1.8 What are the topics that are the most challenging to tackle for the DPO of the Company currently?

The Company is a firm with 2,850 employees that is developing and implementing changes at a large-scale, policies, procedures, IT measures are constantly being improved to comply with the most recent regulations but also with the highest standards and digitalization.

According to the DPO of the Company, the most challenging topic to tackle is change management. The company is developing the most efficient tools and standards to ensure data protection but like for any other company regardless of its size, the changes have to be understood and applied by the employees of the firm dealing with personal data. The employees of the Company have to be aware of the data protection and to make the people accountable for the personal data they process.

4.1.9 In Luxembourg where the financial sector is the main activity, is it an additional challenge for the DPO of the Company?

The core of the activity of the Company is to work with companies, it is qualifying as a business-to-business activity. Most of the companies to which the Company provides its services are professional of the financial sector, therefore the activity of the Company is indirectly related to the financial sector.

According to the DPO of the Company, the specificities of the financial industry have an influence and shall be considered in the data protection strategy of the firm. However, this is mostly driven by the business-to-business activity of the Company where the clients of the firm have also their own customers' and their own employee's personal data. This is not a challenge but something that the Company is attentive to.

4.1.10 Does the DPO of the Company work together with other DPOs in Luxembourg to align practices and create market practices?

The DPO of the Company is personally a board member of the association for the data protection in Luxembourg (APDL), however besides the guidance from the CNPD to develop market practices, there is no official association including a wide selection of stakeholders of Luxembourg working together to align their practices with regards to personal data.

4.2 Risk Based approach

4.2.1 The Company has implemented a DPIA methodology did the DPO get inspiration from the methodology developed by the CNIL or the ICO?

The ICO is the UK data protection authority.

The DPO of the Company specifies that the Company has developed its own DPIA methodology in correlation with its the severity breach assessment. It is understood that where a data breach would occur, the assessment of the severity breach takes into consideration the impact assessment that is performed on the process.

4.2.2 How does the DPO assess severity of a breach? With the development of a methodology inspired from the ENISA's?

The DPO discloses that the Company has developed its own methodology to analyse the severity of a breach. The assessment conducted by the Company is inspired from the recommendation of the CNIL and has for purpose to identify whether the data breach presents a risk for the confidentiality, integrity or availability of the data.

As a closing statement to this conversation, the DPO of the Company highlights that of his opinion, the GDPR should not be perceived as a burden for companies but as a path to value the personal data that they process.

5 Table of references

5.1 Regulations and directives and texts:

Regulation 2016/679
Regulation 648/2012
Directive 2018/843 amending the Directive 2015/849
Luxembourgish Trade Code
Luxembourgish law 1 August 2018
Directive 2014/91/EU
Directive 2011/61/EU
Directive 2004/39/EC
Directive 2014/65/EU
WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of the GDPR, last revised and adopted on 4 October 2017

5.2 Websites:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
https://cnpd.public.lu/fr/actualites/national/2018/11/violation-donnees.html
http://legilux.public.lu/eli/etat/leg/loi/2002/08/02/n2/jo
https://www.iso.org/isoiec-27001-information-security.html
http://data.legilux.public.lu/file/eli-etat-leg-loi-2018-08-01-a686-jo-fr-pdf.pdf
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=FR
http://legilux.public.lu/eli/etat/leg/loi/2018/02/13/a131/jo
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
https://www.enisa.europa.eu/publications/dbn-severity
https://cnpd.public.lu/fr/actualites/national/2018/11/violation-donnees.html
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf
https://cnpd.public.lu/en/professionnels/obligations/AIPD.html
https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf
https://cnpd.public.lu/en/professionnels/obligations/AIPD.html
https://cnpd.public.lu/content/dam/cnpd/fr/legislation/droit-lux/doc_loi02082002_en.pdf
https://cnpd.public.lu/content/dam/cnpd/en/legislation/droit-lux/doc_loi30052005_en.pdf
https://cnpd.public.lu/content/dam/cnpd/fr/actualites/national/2018/formation-cnpd-intro-pd/en-3-obligations-du-rt.pdf