The GDPR and its impact on personal data management

COPENHAGEN BUSINESS SCHOOL
Master Thesis 2018 Cand. Merc IT.
Supervisor: Associate Professor Jonas Hedman

Authored by:
Andreas Boris Hald – 28528
Carsten Leth Svaneborg – 14923

Date: 14/5-2018

Pages: 73
Characters: 145.465

“In God we trust, all others must bring data.”

W. Edwards Deming

Abstract

In a world of an ever changing regulatory environment, companies are finding themselves under increasing regulatory pressure. Most recently the European Union passed the General Data Protection Regulation (GDPR), which seeks to improve and standardise the data protection and privacy of European citizens. We investigate how these standardisations promote personal data management processes outsourcing for financial institutions. Using an explanatory case study approach with multiple larger financial institutions, this thesis qualitatively examines how the GDPR has affected outsourcing of personal data management. Using theories from the Transaction Cost Economics field, we have developed a conceptual framework which aims to illuminate the previously unexplored field of regulatory outsourcing. Through semi-structured interviews with experts from Danske Bank, Jyske Bank, Nordea and Nykredit we have explored how the GDPR affects outsourcing decisions in larger financial institutions.

Through our analysis, we explored the impact of the GDPR on transaction properties such as asset specificity and uncertainty. We saw that asset specificity has appeared to decrease, however not the the point where the market becomes more efficient than internal production. A possible explanation for the lack of outsourcing could be the increased level of uncertainty, which we also observed.

Conclusively, the findings revealed that the GDPR has had no effect on outsourcing for large financial institutions and we observed that it had little to no effect on the decision to outsource.

Acknowledgements

We would like to thank all the organisations that chose to participate in this study; Danske Bank, Jyske Bank, Nordea and Nykredit. We understand that the GDPR is a big undertaking for them, and we are humbled by their acceptance and willingness to participate in our study. Furthermore, we would like to thank the individuals from each organisation who took time out of their busy schedule to speak with us, even so close to the deadline of the General Data Protection Regulation entering into effect.

- Jens Klæbel, Danske Bank
- Sjanna Evers Spliid, Jyske Bank
- Ellen Pløger, Nordea
- Hanne Roliggaard Andersen, Nykredit
- Simon Frank Wendelboe, Nykredit

We would also like to thank Copenhagen Business School for being an institution of higher learning, and allowing us to grow and broaden our horizons through the past five years.
Our thesis counsellor Associate Professor Jonas Hedman, also deserves a special mention for guiding and helping us through this process.

Andreas Boris Hald

_____

Carsten Leth Svaneborg

_____

Table of Contents

Introduction

The regulatory landscape regarding personal data management has been changing for years. With the rapid expanse of the internet, and related services, these regulations have gotten more and more focus. In the last couple of years, the General Data Protection Regulation (GDPR) has contributed to the huge media attention on personal data protection and data privacy. (Badshah, N. 2018).

Since 1995, the European Union has had the Data Protection Directive, to protect the privacy and data security of the citizens of the European countries. This legislation has ensured that citizens in the European Union have enjoyed some of the highest standards of privacy and data protection in the world (Butterworth, 2018). The Data Protection Directive of 1995 has been implemented in Danish legislation as the Personal Data Law (Persondataloven). This law is responsible for protecting the privacy rights of Danish citizens until it is superseded by the GDPR on the 25th of May 2018.

The European Union increased the protection of citizens and in 2016 passed the GDPR, which will replace the Data Protection Directive as the regulation that protect privacy and personal data in the European Union. The new regulations will be updated to also reflect the modern age of the internet, e.g. by tackling the issues of data profiling, informed data consent and increased ownership of personal data.

Notably. the GDPR is a European regulation and not only a directive. Briefly, this means that the data protection regulation will be unified across the European Union as opposed to today, where each country has implemented their own version of the Data Protection Directive of 1995, illustrated by the Danish "Persondatalov". We will expand more upon the consequences of this in the analysis section.

This paper will seek to explore the impact of the GDPR on financial institutions, specifically the impact on the outsourcing aspects of personal data management. We will examine how the changes from the previous directive affect the personal data management processes, and try to explain the consequences of the GDPR. We have interviewed the largest financial institutions in Denmark to examine how they have viewed the GDPR and how they have chosen to handle the challenges it presents.

Outsourcing has, for many years, been a way of reducing costs within companies and organisations (Lacity et al., 2009). And from 2000 to 2014 we saw an explosion in IT outsourcing, while companies have started bringing the competencies back in-house over the last couple of years (Statista, 2017). We seek to explore how this new regulation affect financial organisations, specifically regarding outsourcing and if these changes by the GDPR have changed the potential outsourcing market for personal data management.

This paper will focus primarily on the Danish financial market, by exploring the changes through the largest financial institutions, some of whom are multi-national. The financial sector handles large amounts of personal data, banking information, loan applications and have a high level of trust by the consumers. By focusing on this market, we ensure that we only look at companies that actually handles personal data and will be directly affected by the regulations. The financial sector is known for being heavily regulated, which will ensure that we use data from organisations that are used to handle compliance issues. Furthermore, as the penalties of the new regulations are based on a percentage of annual turnover of the global parent company, larger multinational organisations face a higher risk than smaller organisations. For example, if Google Denmark violates the GDPR, then the whole Alphabet (parent company of Google) might face a 4% fine of annual, global turnover. This ensures the attention and prioritisation of large companies.

We will start this paper by identifying the theoretical knowledge gap, we will research the Transaction Cost Economics theory and use this to build a conceptual framework which we can use to analyse the regulatory changes. Next we will detail our methodology and approach and finalise the section by stating our research question. We will then analyse the collected data and present our findings. Next we will put our findings in the context of our conceptual framework in order to discuss how this can be used to answer our research question. Finally, we will discuss the implications of our findings and put fourth our thoughts on future research possibilities.

Theoretical Framework

As mentioned in the introduction, we seek to analyse the phenomenon of outsourcing through the impacts of the GDPR. Our initial hypothesis is that the GDPR will impact the costs and processes of personal data management. Throughout this section, we will describe the theoretical foundation of this paper and outline how and why we seek to explore this phenomenon. We will start with an examination of the literature relevant to firms' motivation for IT outsourcing to give us an understanding of the present knowledge in the academic field. Furthermore, we will examine Transaction Cost Economics (TCE) starting with 'The Nature of the Firm' by Coase (1937) and leading to when Williamson (1981) created the TCE theory. We will look at relevant confirmative studies to critically reflect upon the theory in order to ensure we have a broad understanding of the scientific consensus regarding the theory. We will then use this examination to build a conceptual framework with which we then use to analyse the impact of the GDPR on outsourcing of personal data management.

Throughout this paper, we will use the terms general, specific, explicit and complex relating to either the business and legislative context or to the outsourcing theory context. The confusion is especially present with the word 'specific' since it has a meaning in the outsourcing literature that can vary greatly from the original meaning of the word and may lead to confusing sections. Therefore, we have chosen to define two different areas for two sets of words.

When we are discussion specificity in relation to outsourcing theory, then we will use the terminology, as defined by Williamson (1981), where 'general' and 'specific' are the two extremes on a spectrum. *Specific* in this context refers to the degree of a process being specific (or unique) to a single company, where *general* is the opposite. A general asset is something that is not unique and is used by many organizations, where a specific asset is used by very few organisations.

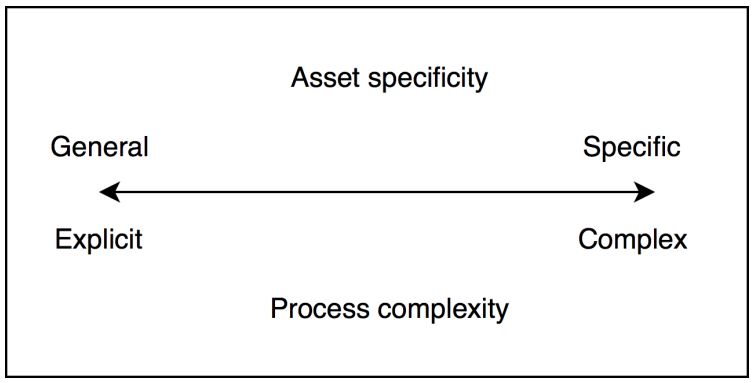


Figure 1 - Relationship between asset specificity and process complexity

The relationship between process complexity and asset specificity is illustrated in Figure 1.

When we discuss a process from a business or legislative perspective then we will use the terminology of explicit versus complex. If a process or asset is explicit, then it must be easier to define and therefore it must make the process more general in outsourcing terminology. And on the other side, if a process or asset is more complex, then it must be harder to define and therefore be a more specific process or asset in outsourcing terminology.

Literary Review

We have initially researched the relevant papers through the CBS library and Google Scholar, to get a better understanding of what motivates firms to outsource. This has led us to 11 relevant studies of motivations for outsourcing. From these 11 studies, we have categorised the results into three categories with themes that occurred frequently throughout the studies. This was done in order to identify the knowledge gap which this paper will seek to fill.

Reasons for IT Outsourcing:

	Cost reduction	Access to new technologies or capabilities	Core Competencies & Competitive Advantage
Currie (1998)	x	x	x
Currie & Willcocks (1998)	x		
Seddon, P.B (2001)	x		
Straub et al. (2008)	x		x
Lacity & Willcocks (2000)	x	x	
Levina & Ross (2003)		x	
Venkatraman (1992)	x		x
Saunders et. al (1997)	x	x	x
Gonzalez (2010)	x		x
Teng et al. (1995)		x	
Loebbecke & Huyskens (2006)	x		x

Table 1 - Reasons for IT outsourcing

Cost Reduction

The most cited reason for outsourcing is due to cost reduction. If a process or individual product is simple or generic enough, then it can be cheaper to procure it from the market, than to produce it within the organisation (Williamson, 1981).
The core of this argument is the economies of scale argument; if the product or process is general enough, then there will be a provider that can benefit from specializing in that process. This would imply, that all non-specific business areas could potentially benefit from outsourcing. (Williamson, 1981).

Lacity et al. (2009) found for IT outsourcing that *"by far, cost reduction was the most common motive identified by researchers"*. While other motivations might also contribute, it is clear to them that the most significant motivation for IT outsourcing is cost reduction.

Venkatraman (1992) examined outsourcing decisions in the paper "*Determinants of Information Technology Outsourcing*" and through multiple regressions analysis he tests multiple hypotheses regarding outsourcing using data from American companies. One of the hypotheses is *"outsourcing is a key strategy that enable [companies to] . . . improve return on equity"*. He finds significant evidence through his analysis to confirm this hypothesis.

Access to New Technologies or Capabilities

Another often cited motivation for outsourcing, is the ability to acquire access to new technologies or capabilities, which is not within the core competencies of the firm themselves. This argument is often tied closely to the cost reduction argument, where it is found to be cheaper to buy competencies and capabilities in the market and spend more on governance costs, than acquiring and train the same competencies and capabilities internally in the organisation.

In the paper "*An Empirical Investigation of Information Technology Sourcing Practices*", Lacity et al. (2000) cites multiple reasons for outsourcing, with one of them being to *"improve technology or technical service"* they also list this as the second most used reason for outsourcing in their study. In the paper they find that organisations can experience a higher quality of service for outsourced IT services. This is because highly specific capabilities can be provided by suppliers which only focus on this particular capability, and thus benefits from shared learning and economies of scale within the IT service supplier.

Teng et al. (1995) examined firms' motivation to outsource through a study spanning 188 companies. In this study they found that firms outsource because the in-house IT capabilities fall short of expectations. This is

highly related to the above point, that organisations may outsource because it is to expensive or difficult to acquire the competencies internally.

Core Competencies & Competitive Advantage

We also found companies wanting to outsource in an effort to focus on their core competencies. As IT became more ubiquitous in modern companies, some companies started to believe that IT was an enabling technology and saw it as a *'cost of doing business'* rather than a core competency (Currie, 1998).

In the paper "*Using multiple suppliers to mitigate the risk of IT outsourcing at ICI and Wessex Water*" Currie (1998), examines outsourcing at the two companies ICI and Wessex Water. One of her findings related to outsourcing at Wessex Water was: *"The advantage of outsourcing was because it focused attention on the core business.*" and in the case of ICI "*The company tended to consider information systems/services and applications systems as being a service rather than a core competency. IT was described as an enabling technology*".

In the paper "*An Empirical Investigation of Information Technology Sourcing Practices*", Lacity et al. (2000) finds multiple reasons for outsourcing. They find that *cost reduction* is a very prevalent reason for IT outsourcing with 80% of participants citing this reason (participants are able to cite multiple reasons). The second highest category was also our second category, relating to technologies and capabilities, where 59% of participants cited as a reason for outsourcing. The third most cited reason, was described as *"jump on the bandwagon"* where participants perceived outsourcing as an industry trend, where they followed. The fourth most used reason was found to be "*Focus business on core competencies; IT perceived as non-core*". 31% of their participants citing this reason. Which substantiates our third category. We argue that our categories relate closely to the findings of Lacity, with the exception of 'jumping on the bandwagon' which we did not find substantiated elsewhere.

Legislation

We found no previous literature regarding legislation being a driver of outsourcing. Blind (2011) investigated the impact of regulations on innovation, and found several links between these two concepts. It could therefore be feasible that new legislation could be a driver of outsourcing.

TCE claims that the specificity of an asset often contributes to the choice between market and firm - outsourcing or insourcing (Williamson, 1981). While legislation traditionally has increased the complexity and by extension the specificity of a product, new regulation is more focused on standardising. With

legislation such as the GDPR, the second Payment Services Directive (PSD2) and similar, we see that processes are standardised across organisations and countries.
Many types of legislation, especially in the financial sector, make requirements of firms. If these requirements are general (i.e. non-specific) then TCE states that the market should be able to gain economies of scale by offering them as services to other firms (Williamson, 1981).

Lacity et al. (2009) has done more than 18 years of research on domestic IT outsourcing and has learned that firms outsource IT capabilities *"mostly to reduce costs, access resources, and focus internal resources on more strategic work"*. This has served as the foundation for our categories. We feel confident that we have successfully identified a knowledge gap, since we found no evidence within the literature suggesting regulatory changes as a driver of outsourcing.

Transaction Cost Economics

In order to understand better understand why firms outsource in the first place, and in order to analyse the data which will be collected through interviews in this study, we have looked back to why firms exists in the first place, why organisations form and how they choose between transacting in the market and within the firm.

The deeper examination of why firms exists begins with R. H. Coase and '*The Nature of the Firm*' from 1937. At the time, economic understanding was primarily focused on supply and demand, and the economic system was understood as an organism coordinated by the price mechanism (Coase 1937). Firms however seemed to violate this, as Coase asks "*Yet, having regard to the fact that if production is regulated by price movements, production could be carried on without any organisation at all, well might we ask, why is there any organisation?*" In the paper Coase finds that the main reason firms exist is that there is an inherent cost of using the price mechanism, namely discovering the relevant price. These costs are called transaction costs and they are inherent in any transaction and most importantly, they do not transfer any value to the transaction. Transaction costs can be seen as friction in a mechanical system, when gears turn towards each other, there is a loss of energy in form of friction between the gears, this is the same in economic transactions, resources being wasted without adding any value. And just as oiling gears and machining them to reduce friction, firms seek to reduce their transaction costs. Coase defines this as "*A firm will tend to expand until the costs of organising an extra transaction within the firm become equal to the costs of carrying out the same transaction by means of an exchange on the open market, or the costs of organising in another firm*."

Coase (1937) began by asking questions about why firms sometimes decided to use the market as opposed to creating products or services themselves, and his theory laid the foundation for outsourcing as we know the concept today. A more detailed examination of the outsourcing concept came with Williamson, who won a Nobel prize for his work with transaction economies (The Nobel Foundation, 2009).

Transaction costs is generally a question of efficiency. Is it more efficient to produce internally in the organisation or is it cheaper to procure it from the market? Generally, markets have an advantages in costs due to their economies of scale (Williamson, 1981), while the internal production is more efficiently governed. The economies of scale advantage is most extreme when the product is general. For more specific products, the economies of scale advantage does not apply to the same degree and there is a higher tendency to insource the production due to significantly lower governance costs (Williamson, 1981).

Williamson (1981) described a simple model for outsourcing, with 4 central points:

- Physical asset specificity is never valued by itself, but only because demand is thereby increased in design or performance respects.
- Such valued demand consequences are often realized only at greater production expense (standardized items would be cheaper because scale economies could be more fully exhausted).
- The optimal choice of asset specificity requires that demand and production cost consequences be taken into account simultaneously.
- Governance costs also vary with asset specificity and these also have to be introduced into the calculus.

Williamson (1981) determined that the choice between firm and market production can be explained by examining three properties of the good being transacted; asset specificity, uncertainty and frequency. This assumption is based on the behavioural premises of bounded rationality and the opportunism of human agents.
Bounded rationality states that people are rational, but their rationality is limited by their capacity to *"formulate and solve complex problems and to process information"* (Williamson, 1981). Opportunism is defined as "*self-interest seeking with guile*" meaning that individuals are willing to provide false information in order to gain advantages when transacting (Alaghehband, 2011).

Asset specificity

Asset specificity is defined as:

> "*the degree to which the assets used to conduct an activity can be redeployed to alternative uses and by alternative users without sacrificing product value*" - Williamson, 2010.

Williamson understands asset specificity as the degree to which an asset can be used in several different places, e.g. if a company requires a very specific drilling machine that is not used by anybody else, then they are the sole demand of that product. The supplier will therefore not be able to use the resources for any other demand. On the other hand, if the drilling machine was a very standard drilling machine, then it would be much more efficient to procure it from the market, as the market has economies of scale efficiencies.

There are three different categories of specificity (Williamson, 1981):

- *Site specificity*, which is related to the geographical position of the good or investment.
  Site specificity could be investing in transportation between a gold mine and the sea. This investment is highly dependent upon the geographical properties of the gold mine. If the gold mine stops producing goods for which your investment can be utilised, your transportation investment cannot be redeployed to utilise a different gold mine, because there are none in the vicinity.

- *Physical asset specificity*, which is related to equipment and tools.
  Physical assets can be all assets involved in production, which also includes IT systems and processes used when doing business.

- *Human asset specificity*, which is human knowledge, learning and skills.
  Human assets specificity can be knowledge, an example could be performing maintenance on a new Mercedes, where specialised training and knowledge is required to understand the machinery, it is not simply a combustion engine on wheels.

Uncertainty

The second critical property of transactions, as described by Williamson (1985), is uncertainty. Uncertainty relates to the uncertainty of the transaction. Transactions with a higher degree of uncertainty carry with them an inherent higher risk, which should be accounted for. Both opportunism and bounded rationality can be a factor in uncertainty. If individuals choose to distort information for personal gain, it can create uncertainty as a consequence of opportunism (Williamson, 1985). Uncertainty can however also be a consequence of

bounded rationality, when transacting with imperfect information (Williamson, 1985). Such a transaction could result in exposure to risk that were unforeseen, or the unwillingness to transact because risks cannot be calculated precisely.

Frequency

Frequency is defined as "*the buyer activity in the market*" (Williamson, 1979). It relates to the occurrence of the action for each transaction. It can be single purchase, acquiring people or equipment, or recurring purchases, acquiring goods or services that factor in the production process. Of the three properties related to transaction costs, Williamson (1979) describes frequency as the property with the least influence on outsourcing decisions.

Production and Governance Costs

There are two types of costs associated with transactions; production costs and governance costs (Williamson, 1981). Production cost (C), is the direct price of producing the good or service either internally or acquiring it in the market. Governance cost (G) is the costs of planning, monitoring and negotiating the transaction. As both terms can relate either within the firm or in the market, we can represent this change as ΔC and ΔG, each representing the change in costs between the firm and the market (Williamson, 1981).

Williamson (1981) depicts the relationship between asset specificity, production costs and governance costs, as seen in Figure 2.

The vertical axis represents the change (Δ) in costs between the market and the firm, a positive value (>0) suggests that the market is more cost efficient and a negative value (<0) represents that the firm is more cost efficient. The horizontal axis, *A*, represents the asset specificity from a general asset (to the left) to a specific asset (to the right).

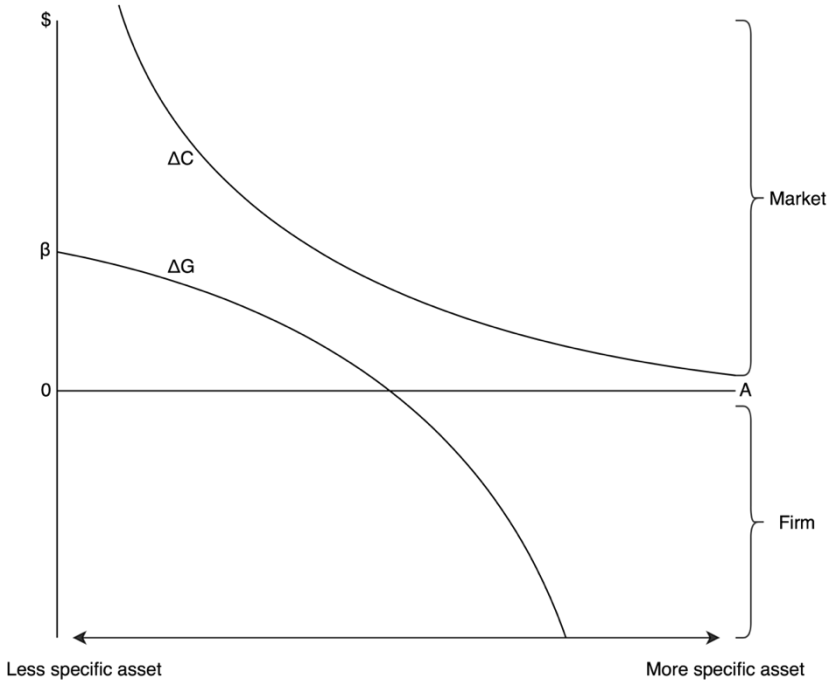


Figure 2 - Relationship between asset specificity, production and governance costs

If we look at the difference in production costs between the market and internal production, ΔC, we see a very clear tendency. Looking at one extreme end of the ΔC, with high asset specificity, we see that market procurement is only slightly more efficient than internal production. One of the main reasons is the fact that the market cannot reuse the resources spent on the very specific asset for other clients. Moving towards less specific assets, we see that the advantage of the market in production costs increases. This is primarily due to economies of scale, where the market is able to reuse the resources for the asset and distribute the costs among multiple clients. At the other extreme end, when asset specificity is very low, we see that the market has a huge advantage in production costs compared to internal production.

The difference in governance costs, ΔG, follows a more interesting pattern. When asset specificity is low, the market has a significant governance costs advantage compared to internal production. This is primarily due to the standardised and general nature of the asset, that it is easily managed and governed. Governing the production of a standard asset is less efficient internally, as all of the governing costs are taken by the firm itself. The more specific an asset becomes, the less efficient the market is compared to internal production until the governance advantage shifts towards the internal production. The reasoning is that at some point of asset specificity, the coordination within the firm becomes more efficient than external coordination for governing transactions. It is worth noting, that the governance cost difference, ΔG, can be negative (thereby being cheaper to govern internally), while ΔG + ΔC is still less than zero, due to the market still have economies of scale advantages that are larger than the governance advantage.

If assets are general, markets enjoy advantages in both production costs and governance costs. Markets can also aggregate uncorrelated demands, thereby enjoying economies of scale and risk-pooling benefits (Williamson, 1981). However, as assets become more specific, the aggregation benefits of markets are reduced, and any exchange takes on a stronger bilateral character

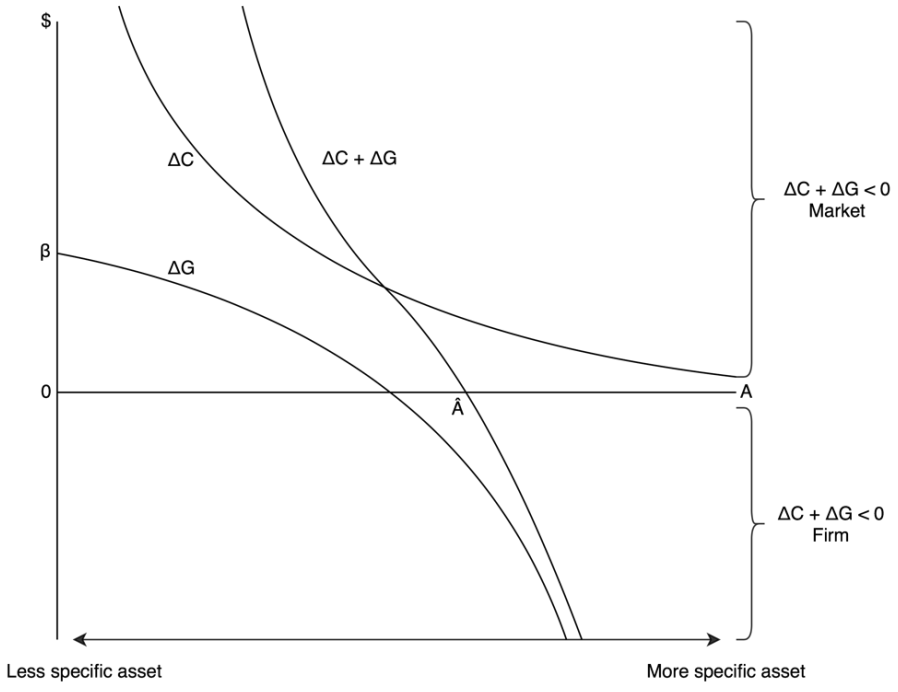


Figure 3 - Change in production and governance costs in a single function

(Williamson, 1981). This leads to an increase in governance costs for transactions. Organisations will tend to replace markets with internal procedures as assets become more specific (Williamson, 1981).

When the asset specificity reaches the point where $\Delta C + \Delta G = 0$, this point is called the point of indifference (Â). At this point the firm is indifferent between producing the asset internally or procuring it externally.

As both ΔC and ΔG are affected by the asset specificity, we can combine them into the function $\Delta C + \Delta G$, as seen in Figure 3. This function describes whether or not a given company should transact within the firm or in the market.
As long as $\Delta C + \Delta G$ is larger than 0, then the theory suggests that market procurement is the most efficient method. When $\Delta C + \Delta G$ is less than 0, then internal production is most efficient (Williamson, 1981).

If we examine what happens as asset specificity decreases, we move to a point more to the left on the horizontal axis, point A_1. This is primarily due to the market having economies of scale advantages, which is achieved by offering the same asset to many different firms, thereby obtaining a cost advantages over internal production. This is depicted as a higher ΔC, and a production cost advantage for the market. In addition, governance costs decrease as asset specificity decreases, due to contracting and selection is simpler and resulting in simple procurement. This is depicted as a higher ΔG, a governance cost advantage for the market. Following this, a higher ΔC and a higher ΔG leads to a higher $\Delta C + \Delta G$, which at A_1 means that markets are more efficient at producing non-specific assets than internal production. This can be seen in Figure 4, if we decrease asset specificity by moving from point Â to point A_1 the intersection point with the line $\Delta C + \Delta G$ is positive, suggesting market procurement should be utilised.

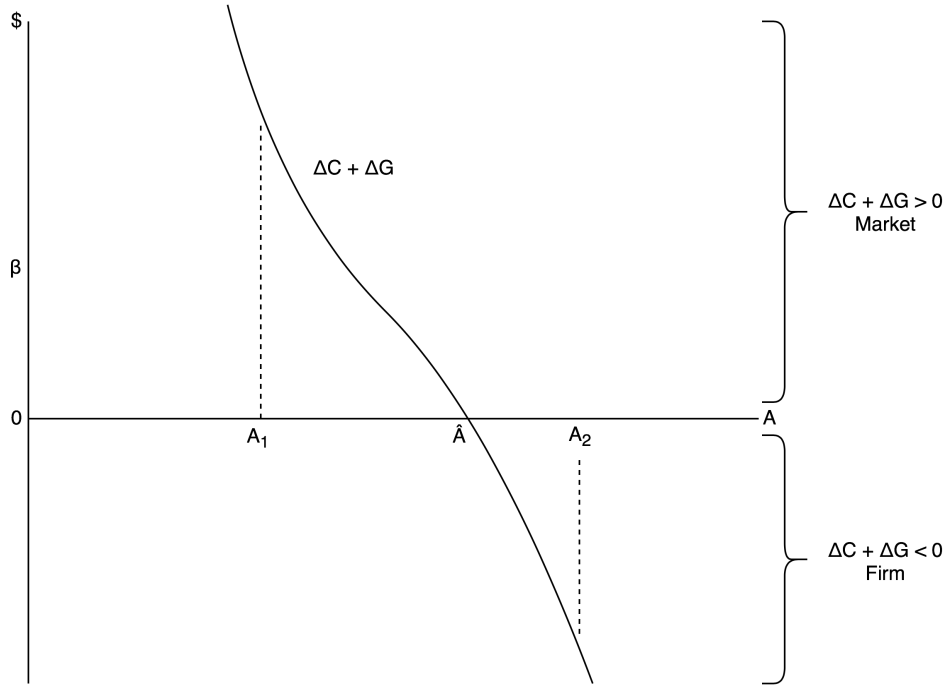


Figure 4 - Changes in asset specificity related to ΔC + ΔG

Conversely, when asset specificity increases from point Â to point A_2, then the production cost advantage of the market becomes more negligible. The governance costs however fall dramatically, because it is much cheaper to govern and monitor internal transactions. This results in the intersection point between point A_2 and the line $\Delta C + \Delta G$ is negative suggesting it is preferable to produce the product within the firm.

Uncertainty and Frequency

In the presence of a certain degree of asset specificity, an increase in uncertainty will reduce the production cost difference ΔC (Alaghehband, 2011). With high levels of asset specificity uncertainty will increase the transaction costs in the market, and decrease transaction costs relatively within the firm. Frequency has a similar effect, however at high levels of uncertainty the effects of frequency is insignificant (Alaghehband, 2011).

The results of uncertainty and frequency can be seen in Figure 5, at the same level of asset specificity Â, the function $\Delta C + \Delta G$ shows an indifference between the market and the firm. However, given an increase in either uncertainty or frequency, all other things held equal, the $\Delta C + \Delta G$ function will shift to the left becoming $\Delta C + \Delta G_1$ (Alaghehband, 2011). Resulting in a stronger preference towards internal production for the organisation. A decrease in either uncertainty or frequency will have the opposite effect, shifting the function to the right (Alaghehband, 2011).

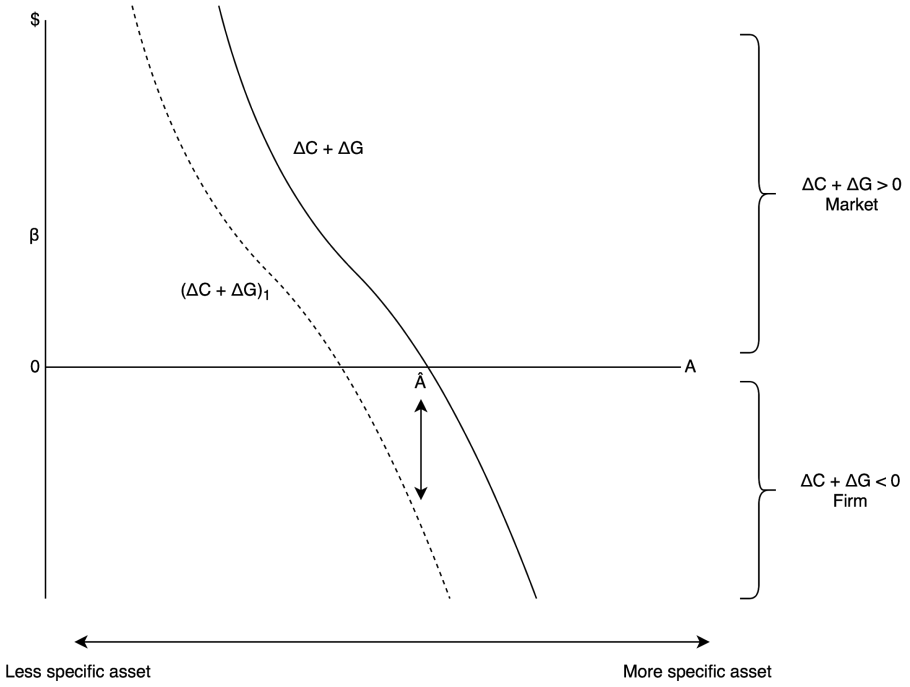


Figure 5 - ΔC + ΔG in relation to uncertainty and frequency

There has been a lot of discussion regarding TCE's empirical validity, as suggested by David et al. (2004) in the paper "*A systematic assessment of the empirical support for transaction cost economics*". David et al. highlight a discussion between Ghoshal, Moran and Williamson about the empirical evidence for Transaction Cost Economics. The paper then goes on to systematically assess literature regarding TCE. The paper details

304 statistical tests based on 63 articles regarding TCE. The results were mixed; 47% supported TCE, 10% were against TCE and 43% showed non significant results.

Carter and Hodgson (2006) argues that: *"There is some significant empirical evidence in support of aspects of TCE, but taking Williamson's analysis and the evidence as a whole, the picture is rather mixed"*. Specifically, they made an empirical review of the studies in the IT Outsourcing (ITO) field where TCE was used. They found five studies that were partial consistent with the TCE framework, five that were partially consistent and inconsistent with the TCE framework and one study that was inconclusive. Their results can therefore be determined as mixed, although more consistent than inconsistent with the TCE framework.

Digging deeper into the results of the statistical analysis by David et al. (2004), they found that the independent variable *'asset specificity'* fared best amongst the independent variables. It was fairly successful in predicting make-or-buy decisions (58%) and was even better at predicting the degree of integration between independent buyers and sellers (79%). This is a specific important aspect of TCE which is highly relevant for this paper.

There is no agreed upon consensus regarding Transaction Cost Economies, and while research continues to find both confirmative and inconclusive results regarding the theory, it is some of the most researched and applied theoretical framework. As Lacity et al. (2011) says: *"Transaction Cost Economies has been the most frequently appropriated theory for the study of IT outsourcing"*. This along with the fact, that David et al. (2004) found that *asset specificity* is relevant in predicting make-or-buy decisions, have lead to us using this theory as the foundation upon which to build our conceptual framework.

Conceptual Framework

As understood by our literary review, firms primarily outsource in an effort to reduce costs, gain new competencies or focus on their core competencies. In spite of this, we found no literature on the potential effect that legislative changes can have on the outsourcing decisions of firms. Throughout this paper we will strive to examine how legislative changes can motivate firms to outsource systems or processes. This paper will primarily be based on the new General Data Protection Regulation, which has imposed several new restrictions to how organisations operate in regards to personal data management.

New legislative requirements can have an impact on the compliance costs with the legislation (Blind, 2011), which we will examine further in regards to the GDPR.
Extrapolating from the TCE theory, it is clear that if the new legislation lowers the specificity of compliance with the legislation, then it would (1) shift the advantage of the difference in governance costs towards the

market and (2) increase the difference in production costs as a result of a potential increase in economies of scale, which would further enhance the advantages of the market.

The costs of procuring from the market would therefore fall in relation to the costs of producing within the firm (Williamson, 1981). This should lead to more companies outsourcing the competencies or processes required to be compliant with the legislation.

We have modified Williamson's simple model of Transaction Cost Economics, in order to better examine these legislative changes:

1. The specificity of an asset, process or product can be increased or decreased by legislation.
2. Decreasing the specificity of a process should result in:
    a. An increase in the difference in production costs ΔC
    b. An increase in the difference in governance costs ΔG
3. An increase in ΔC + ΔG to a point above Â (Figure 6), should result in an increase of market procurement for that process

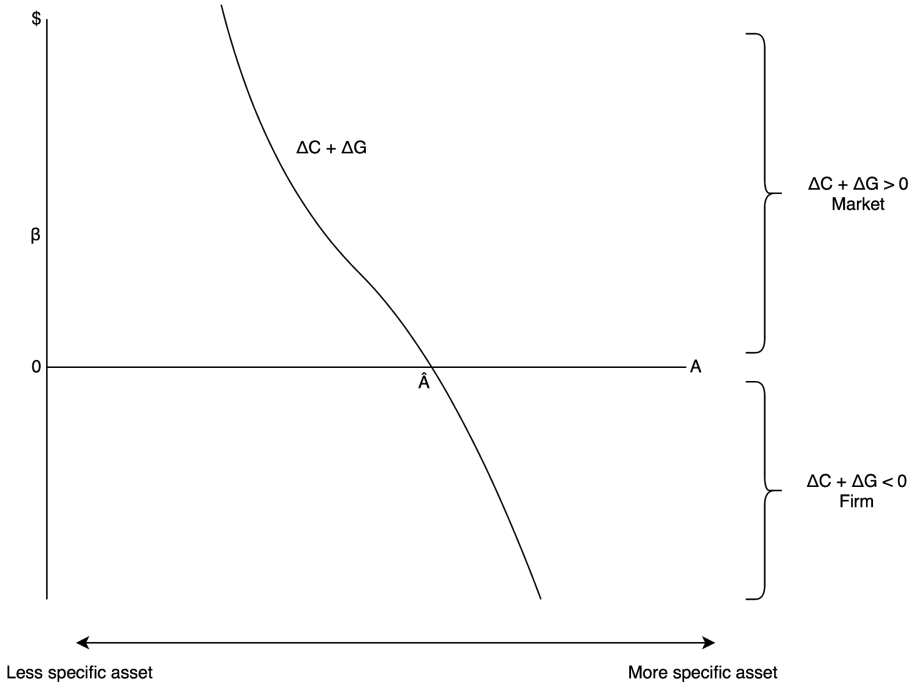


Figure 6 - Conceptual Framework Model

Methodology

For this section, we will present our methodology, our general approach throughout this paper and our reasoning behind our choices. We will start by explaining our research process. Afterwards, we will present the choice of organisations that we have examined. Next we will dive into our research design by explaining how we collected the data for this paper, including a section on the interview guide and our reasoning for the questions within. Then we will present the interviewees to give the reader some background knowledge of the context we interviewed in. Furthermore, we will have a section on how we have analysed the data. These sections will lead us to our research question. And finally we will examine the reliability, validity and generalizability of our study.

Research Design

In the following section we will clarify the research design with which we have chosen to approach this research. We will seek to describe in, as much detail as possible, the process we have used and explain our reasoning as to inform the reader and to increase the replicability of the study.

When formulating the research design of this paper, we have decided to adopt an explanatory approach. This approach is described where "*emphasis is on studying a situation or a problem in order to explain the relationships between variables"* (Saunders et al. 2016). We therefore seek to study and explain the relationship between the GDPR and outsourcing in large financial institutions.

This approach also allowed us to study the reasoning of the organisations that choose to outsource or not to outsource particular aspects of the GDPR, which would be relevant given the explanatory nature of the paper. Our strategic research approach to this was to use case studies, to study the phenomenon. Saunders et al. (2016) uses the definition of a case study as *"a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence"*. We use this definition since the contemporary nature of the problems concerning the GDPR, and our approach to analyse multiple financial institutions solutions of this issue. An explanatory approach is especially useful when seeking a deeper understanding of the context of the research and the process being enacted (Saunders et al. 2016). We argue that we first need to obtain a deep understanding of the legislation both in context to itself, but also in a historical setting. Secondly, we need to obtain an understanding of how each organisation have chosen to solve these complex issue introduced by the legislation, in order to understand if, how and what have been outsourced due to regulation in relation to our conceptual framework. Furthermore, this research is made as a cross-sectional study. This is a 'snapshot' of

the reality and is best used to understand the current situation (Saunders et al. 2016), this will be further discussed in the discussion section of the paper.

Review of literature

The main purpose of reviewing relevant literature is to develop a deeper understanding of what other researchers have been doing in the same field (Saunders et al., 2016). It is crucial to review all relevant literature to ensure you have a deep and broad understanding of the subject matter. Outsourcing has been very well studied and relevant literature were easy to come by. We have used a mix of direct literature on outsourcing and reviews of the outsourcing literature. Some of these reviews include '*Models referring to outsourcing theory'* by Vaxevanau et al. (2014) and '*Business Process Outsourcing studies, a critical review and research directions*' by Lacity et al. (2011).

There are two different approaches for reviewing literature, an inductive and deductive approach (Saunders et al., 2012). The inductive approach is related to exploring your data and using it to build theories that can be related to the literature. The deductive approach, upon which this paper is built, is meant to identify theories in the literature that can be used to create a conceptual framework, from which the data can be tested upon. This is the approach taken within this paper, where we in the literature review define and research outsourcing literature to define the theory and identify the knowledge gap. We have used this knowledge gap to create our research question, and the outsourcing theory TCE, to create our conceptual framework which we seek to test using the data collected through this paper.

Choice of Organisations

We have chosen to do a study of the large financial organisations in Denmark. Our reasoning for choosing the large financial institutions is primarely because they are big enough to make independent decisions about how and what processes they will follow. Very specific markets or areas are also ideal for examining the impact of regulatory changes (Blind, 2011).
Almost all of the Danish banks are using one of the three major software providers for the Danish banking industry, being SDC, BEC and Bankdata. The smaller banks are mostly using a white-label solution for their infrastructure, where the larger banks are developing more independently. We therefore selected the larger banks to see whether or not, regulatory changes have enabled personal data management to be outsourced. There is also a case to be made, that the smaller banks could be looking for inspiration in the larger banks. The size of the financial institutions was therefore our main selection criterion. The Danish Financial Service Authority (*Finanstilsynet*) each year publishes a report of the largest financial institutions in Denmark, measured on their total assets. The category with the largest financial institutions, was defined as those

institutions with a working capital of more than 75 billion DKK. In 2017, there were four banks on this list (in descending order):

- Danske Bank A/S
- Jyske Bank A/S
- Sydbank A/S
- Nykredit Bank A/S

However, the list from 2016 also included Nordea, which was excluded from the list in 2017 due to their legal restructure. We have decided to include Nordea in our study, as they would be the second largest financial institution in Denmark if measured by total number of customers. We invited all five financial institutions to participate in our study, with four of them accepting the offer. Therefore, our study consists of interview data from the following four financial institutions, ranked by size:

- Danske Bank A/S
- Nordea Bank AB
- Jyske Bank A/S
- Nykredit Bank A/S

As we have been able to collect data from four out of five of the organisations in the targeted market, we argue that we have succeeded in collecting a large enough sample size for it to be representative of the larger financial institutional market in Denmark.

Data Collection

The GDPR is going into effect on the 25th of May. The GDPR was written into law in May 2016, however there is a two-year grace period before legislation enters into effect in the EU. Therefore, we have an initial assumption that the organisations have been working and preparing for the legislation to take effect. Because of this we wanted to utilise an explanatory strategy, so that we may discover which approach each organisation has taken to become legally compliant before the deadline.

The data we needed for this thesis was qualitative data. Therefore, we needed to keep the interviews open but we still needed to have some control over the interview. The semi-structured interview format was chosen, as this allowed us to phrase the initial interview questions. This allowed us to remain in control while letting our interviewees speak freely. In practice, this was done through an initial open-ended question, where we would use follow up questions to further explore the subject. This allowed us to not only see *how* the

organisations have handled the legislative changes, but more importantly *why* they have handled it as they did.

Kvale (2007) also emphasises the importance of understanding the subject matter before the interviews, as to better be able to follow up with meaningful questions

> "*Without any presentation of the existing knowledge about the topic of an investigation, it is difficult for both researcher and reader to ascertain whether the knowledge obtained by the interviews is new, and thus what the scientific contribution of the research is."* Kvale (2007).

Therefore, the initial part of this paper seeks to introduce the GDPR to the reader, but also to show that we, as researchers, have studied the particular legislation fully in order to better interview our interviewees.

Our approach has been to extensively review the literature regarding TCE, upon which we have built our conceptual framework, and to research the GDPR legislation. This review allowed us to conduct meaningful interviews with questions that both seek to answer a theoretical aspect of our conceptual framework but is also specific to the legislation and the situation of the organisation.

The collecting data has been transcribed and can be found in the appendices (appendix 4-7). As the interviews were conducted in Danish, they were also transcribed in Danish to preserve the authenticity of the interview. Statements used in the paper were then translated to English. For the interview transcriptions, a simple notation is used. At the top of each interview, all participants are listed and assigned a single letter to indicate who is talking.

We have concluded every interview with a 'debriefing' as recommended by Kvale (2007). This is the concluded part of the interview where the interviewer can ask for feedback on the interview and ask if the interviewee has anything more to add. This can be done by summarizing the interview to see if the subject has further comments on any specific insight that was obtained. This can for example be seen in the interview with Danske Bank (Appendix 6) where at the end of the interview we asked *"Do you have anything else you feel is relevant for us to know in relation to the GDPR"*, which then sparked additional discussion.

Interviewguide

When evaluating interview questions, it should be done with regards to two separate themes; thematically and dynamically (Kvale, 2007). Thematically, the questions should seek to answer questions relating to the theoretical aspect of the interview that is being conducted. The questions should therefore be considered in regards to the analysis to be performed afterwards. If coding of the interviews is to be utilized, it can be beneficial to clarify the meaning of the subjects' statements in regards to the categories to be used in the coding process. However, if a narrative approach is used the interviewer should give the subject ample opportunity to elaborate and time to unfold their story. For this thesis, we have chosen to categorize our interviews, which we have designed our interviews accordingly.
Dynamically relates to the 'how' of an interview. Questions should seek to promote interaction and communication between the interviewer and interviewee.
For interviews in general, questions should be kept short and precise, while keeping academic language to a minimum (Kvale, 2007).

It is desirable to have two versions of the interview guide, one meant for the interviewees and one for the researchers (Kvale, 2007). We therefore created two separate interview guides, one which we sent to the participants and described the questions in more general and layman terms and another version we, as the researchers, used during the interview. The version we used in the interviews contained our own follow-up questions, which we defined based on the range of possible answers. Planning for every possible response is impossible, so we tried to plan for both the expected answers and then also for the opposite of the expected answer. Then we would have questions for both ends of our expectations and therefore also be prepared for answers that lie in between the two extremes. Completely unexpected answers were examined on the spot. An example of this is the question *"Have any processes or capabilities been outsourced in order to be compliant [with GDPR]?"* which could either be followed up with *"What factors were evaluated in your decision to outsource?"* or *"Was outsourcing considered?"*.
This aided us during the interview, as we could ensure, that no important follow-up questions were missed. The researchers' version of our interview guide can be found below, while the interviewees' version can be found in Appendix 3.

Introduction

- Who are we?
- Why this study?
- Expected outcome

Personal Information

- Position/Title and department
- Experience and history within the organisation

GDPR

- What has your organisation done with regards to the GDPR?
    - Get a thorough understanding of the individual organisations process.
- Do you expect that your organisation will be compliant with GDPR before the deadline?
    - If yes, how automated will the different processes be?
    - If not, what is the timeline?
- How has your organisation reacted to the GDPR?
    - Clarify major or minor undertaking.
- Have any processes or capabilities been outsourced in order to be compliant?
    - If so, what factors were evaluated in the decision?
    - If not, was outsourcing considered?
- Has other organisations approach to GDPR compliance influenced your decision?
    - If so, which and how?
- Additional comments that could be relevant?

We started each interview with some introductory information, both relating to us as researchers and the background for this particular study. This was suggested by Kvale (2007) who recommends when beginning an interview, the interviewer start by introducing himself and the study, whilst defining the situation for the interviewees and answering any preliminary questions that might arise.

The next section of the interview is focused on the particular interviewee, to ensure that they have the relevant position and knowledge within the bank to speak in detail about the GDPR ramifications. This was particularly relevant in the Nykredit interview, where Hanne Roliggaard Andersen, who has deep knowledge of a particular department's implementation of GDPR, brought in a colleague, Simon Frank Wendelboe, to talk about the technical and organisation-wide aspects of their GDPR implementation.

After the initial clarifying parts of the interview we move on to the actual questions of the interviews. These were formulated in layman's terms so that everybody could understand them, in accordance with Kvale (2007). The follow up questions are formulated to ensure that relevant data is captured.

An example of follow up questions and process can be seen during the interview with Ellen Pløger from Nordea (Appendix 5), where the following question was posed:

> *"If we look at some of the competencies it has required both IT and regulatory (...) is it something you have had internally, or have you had to look externally to consultants or systems?"*

Her very detailed answer focuses primarily on the regulatory side, which prompted the following question:

> *"The relevant IT systems, is that something you have developed internally? Or was it purchased externally?"*

This allowed us to make sure that all relevant information was captured, so we later could analyse the responses and categorise them according to our categories.

Interviewees

For this section, we will briefly introduce the financial institutions participating and the interviewees that represents them. This is done to align the readers background knowledge with the researchers' background knowledge.

Organisation	Name	Position	Date	Form	Transcribed
Danske Bank	Jens Klæbel	Senior Vice President - Compliance Programme Office	4/4-2018	Meeting at Danske Bank	Appendix 6
Jyske Bank	Sjanna Evers Spliid	Data Protection Officer	27/3-2018	Telephone	Appendix 4
Jyske Bank	Majken Christoffersen	Lawyer - Legal	30/4-2018	E-mail	Appendix 4
Nordea	Ellen Pløger	Group Data Protection Officer (DPO)	11/4-2018	Meeting at Nordea	Appendix 5
Nykredit	Hanne Roliggaard Andersen	Digital Marketing department, GDPR department responsible	20/3-2018	Meeting at Nykredit	Appendix 7
Nykredit	Simon Frank Wendelboe	Project Management Officer, GDPR program	20/3-2018	Meeting at Nykredit	Appendix 7

Table 2 - Interviewees

Danske Bank is the largest Danish banking institution (Finanstilsynet, 2016) and was founded in 1871. It has its headquarter in Copenhagen and spans most of the Nordic countries, some of the Baltic countries and Ireland. Jens Klæbel has been with Danske Bank for the last 20 years. With the official title of Senior Vice President, he is the head of several compliance programmes, among these are the Anti-Money Laundering (AML) programme and the GDPR programme. He has a background in Computer Science from Copenhagen University and has spent 12 years teaching at Copenhagen Business School.

Jyske Bank is the third largest bank in Denmark (Finanstilsynet, 2016) and was founded in 1967 by the merger of four smaller banks with the headquarter located in Silkeborg. Sjanna Evers Spliid is the DPO in Jyske Bank. A DPO is a position required by the GDPR where the individual is responsible for overseeing the company's personal data protection strategy and implementation, and ensuring the organisation is in compliance with the regulation. Sjanna Evers Spliid was therefore the perfect contact point for our thesis. During our follow up questions, Sjanna Evers Spliid was unavailable. However, she put us in contact with Majken Christoffersen at Jyske Bank, who could answer our follow up questions by email.

Nordea is the second largest banking institution in Denmark (Finanstilsynet, 2016). On a European level, Nordea is 14th largest bank (TheBanks.eu, 2016), spanning across the Nordic countries, Poland, Russia and more. It was founded between 1997 and 2000 by the merging of several Nordic banks. Ellen Pløger is the Group Data Protection Officer (DPO) in Nordea and is therefore responsible for the compliance of GDPR for the entire Nordea. She has been with Nordea for more than 30 years. She started out in a business role at Nordea, but in the recent years she has moved towards a compliance profile before achieving the role of Group DPO. Ellen Pløger has a cand.polit degree from Copenhagen University. As Ellen Pløger had the overall responsibility of the GDPR compliance within Nordea, she was the ideal candidate to interview.

Nykredit was founded in 1851, and is the fifth largest bank operating in Denmark (Finanstilsynet, 2016), and has its headquarter in Copenhagen. The bank primarily focuses on mortgage and investment banking and the Nykredit Group is the largest lender in Denmark. We were fortunate enough to receive interviews with two employees in Nykredit.
Hanne Roliggaard Andersen is employed in the digital marketing department of Nykredit. She has been at the bank for more than 16 years with the primary focus area being marketing and CRM. Nykredit has appointed a head of GDPR implementation within each department, and Hanne Roliggaard Andersen was appointed within her department.
Simon Frank Wendelboe is part of the GDPR programme at Nykredit. The programme is responsible for the overall coordination, development and implementation of the solutions regarding GDPR. This includes the communication with each department's head of GDPR implementation, such as Hanne Roliggaard Andersen. Simon Frank Wendelboe has been in Nykredit since 2008.

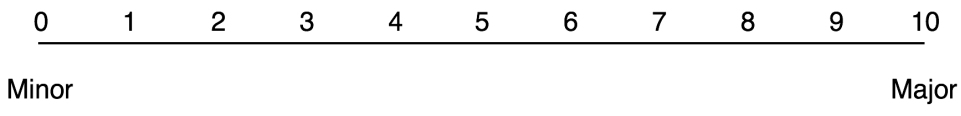
Data Analysis

Kvale (2007) divides the analysis into two parts; analysis focused on the meaning and analysis focused on the language. For this thesis, we will focus on the analysis of the meaning of our interviewees. Similarly, Saunders, et al. (2016) advocates using pattern matching and categorisation. Pattern matching involves creating a conceptual framework to explain our findings. We then test our gathered data against our conceptual framework, to either prove or disprove our hypothesis.
When analysing meaning Kvale recommends coding or categorisation of the meaning in the interview. Coding an interview is attaching one or more keywords to text segments in order to identify the meaning of the statements. Categorisation is defined as the act of reducing complex text segments to a few simple categories. Each statement can then be categorised as either positive or negative towards that category. The strength of the statements tendency towards one or another category can also be expressed with a simple numerical scale, in order to better quantify the interviewee's opinion towards that category. Categorisation can thus help to reduce large amounts of text into figures and tables, and thereby better quantifying the data (Saunders, 2016; Kvale 2007).

We will now describe each categorise and justify why this category was created and how it is scored.

Size of undertaking

Our first category relates to each organisations opinion on the size of the task, being compliant with the regulation. As we felt it would be extremely difficult to define how each organisation should calculate the direct costs of their GDPR implementation. The reason being that each organisations solution to GDPR could vary heavily from each other, and we would have no way of defining this before we started the interview. Furthermore, direct information relating to costs may not be readily available during the interview, and may also be proprietary information. Instead we instead decided to let them define the task on a numerical scale from 0 - 10, with 0 meaning only a minor undertaking, and 10 being a very large undertaking.

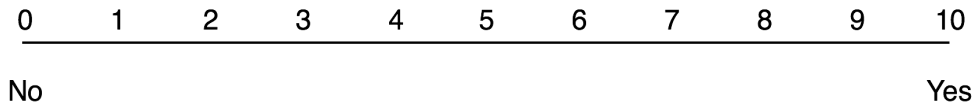


An example of a question formulated during an interview to answer this category can for example be found in the interview with Nordea where the question was posed: *"If you were to categorise the GDPR project, has it then been a very large undertaking? Or has it been a smaller thing because the demands have been*

very similar to what they used to be?". As Kvale (2007) suggests we inform the interviewee that this should be categorised, but posing the question void of any academic language and in an open fashion as to encourage a deeper explanation of the issue.

Outsourced competencies

Our second category relates to whether or not the organisation has outsourced competencies, capabilities or systems relating to GDPR compliance. We discussed having this category as a simple binary yes / no category, but decided on implementing the same scale as in the previous. This was done if organisations decided to implement very different solutions, then they could potentially outsource very different things. So this scale represents how large, or how much, they have outsourced in relation to GDPR. It also encouraged further discussion of the outsourcing process.



An example of a question posed could be: *"If we look at some of the competencies, it has required both IT and regulatory (...) is it something you have had internally, or have you had to look externally to consultants or systems?"* the question was posed this way at the Nordea interview to spark further discussion about what kind of external help was acquired and to what extent, which Ellen Pløger from Nordea (appendix 5) then goes into further details about.

The category relates directly to how the organisation chose to handle the GDPR process, by either outsourcing or handling all processes inside the firm. This relates to the conceptual framework, in that it provides an indication of whether or not the organisation is above or below the point of indifference, Â.

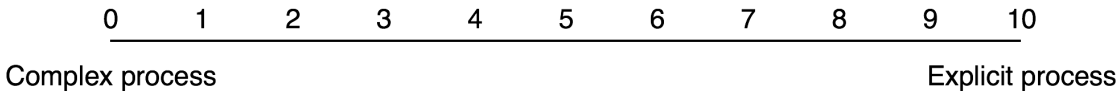
Considered outsourcing?

The next category is closely tied to the previous category, and is only relevant if the organisation chose not to outsource. It classifies whether or not the organisation even considered outsourcing as a possible solution. The category uses the same scale as previously from 0-10, from no to yes. We did consider the fact that our interviewee's may not know or be aware of such a consideration as it may be made at a higher point in the organisation than they were positioned. This however was not a problem, and we were fortunate enough to get interviews with individuals that were directly involved with the GDPR process. The only exception being Jyske Bank where the question was answered by a colleague in a follow-up email.

The category is relevant because it speaks to the organisation's attitude towards outsourcing even if they are below the point of indifference, Â.

Specificity of compliance

This category relates to how the specificity has changed in relation to outsourcing aspects of compliance with the legislation. We will also analyse the legislation itself, but we found it prudent during our interviews to ask our interviewees how they felt the new legislation have changed the explicitness of the legislation. We have chosen to use the same scale as previously from 0 (complex legislation) to 10 (explicit legislation). Their response on the explicitness can be used to indicate whether the GDPR has made the personal data management processes less specific, in an outsourcing context.



Legal changes as a driver of change

This category was added, because during the explanatory interviews, we found that some of the organisations tended to use the GDPR as a reason to defend IT spending for 'cleanup'. This was not directly relevant for the analysis given our conceptual framework, it was however an interesting finding that could spark further research, which is why we decided to include it in the discussion section of this paper.

These categories provide the basis of the information that we extract from our interviews. We will use these categories to analyse our conceptual framework in the later sections.

Research Question

The explicitness of the General Data Protection Regulation, have increased the rights of the data subjects with regards to their personal data. These rights are now more explicitly expressed than previously. The requirements for being compliant with these rights is now more generalized across organisations. From an outsourcing perspective, this means that the specificity of personal data management has decreased, which leads us into a research question that follows:

To what extent has the decreased specificity of the General Data Protection Regulation promoted outsourcing of personal data management in large financial institutions?

Reliability, Generalizability & Validity

It is important to acknowledge the complex nature of a qualitative study. The research may therefore not be easily replicated with the exact same findings, as the findings are qualitative in nature. This is opposed to a quantitative study, where the evidence might be based on a larger empirical data set. However, we argue that since our analysis has covered a majority of the selected market (large financial institutions) and furthermore our interview data is available in this paper, the reproducibility should be high. It should however be noted that the contemporary nature of our findings, will only make our results reproducible in a given timeframe, as time passes the organisations may adapt other approaches to compliance.
Improving the reliability of the study could be achieved through interviewing additional financial institutions. However, as this is a quantitative study depth is more important than width. As argued in the section *Choice of Organisations*, interviewing four out of the five largest financial institutions in Denmark is deemed satisfactory to achieve a high degree of reliability for the context that we are examining.

This study has been focusing on large financial organisation in Denmark, which may limit the results to large financial institutions which are located in demographically and technological societies similar to that of the Danish society. It can be difficult to seamlessly generalize the findings on to other industries. Two major reasons underline this caution. The first is that the financial industry is already subject to a lot of legislative requirements, so they already have a lot of regulatory compliance capabilities in-house. This could decrease their cost of adapting their internal procedures as opposed to outsourcing it. Secondly, a lot of rules imposed by the examined regulation might already be covered by different legislation, thereby decreasing the effect it has on their compliance with regulation. This may not be the case it other industries, and therefore caution is advised when generalizing this thesis.

A high degree of validity was achieved by doing lengthy semi-structured interviews where participants were allowed to elaborate on their view points in their own time and fashion. Clarifying and follow-up questions were asked to make sure that the interviewees answered the essential questions throughout the interviews as suggested by Kvale (2007). The interviews lasted between 45 and 90 minutes, which gave us around 4 hours of interview. Furthermore, we have been fortunate enough to receive interviews with a diverse selection of the most relevant people in each organisation with regards to the GDPR implementation (ranging from Head of Digital Marketing to Group Data Protection Officer to the Senior Vice President of the Compliance Programme).

Analysis

In the analysis, we will seek to examine the General Data Protection Regulations more closely, both in an effort to better understand the legislation, but also through a historical context - analysing the changes from the past legislation, the Data Protection Directive. We seek to examine the impact the GDPR has had on the asset specificity in compliance with the legislation. After the examination we will move on to review some of the results and important points that were found throughout our interviews, and finally put these findings in the context of our conceptual framework.

General Data Protection Regulation

The GDPR supersedes the previous Data Protection Directive of 1995. The GDPR is generally celebrated for its improvements to the data privacy and security of the citizens of the European Union. The GDPR significantly increases the uniformity of data protection regulation across the member countries of the EU. This is primarily due to the change from a directive to a regulation.

An EU directive is legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual member countries to devise their own laws to achieve these goals (European Commission, 2017). An EU Directive is therefore subject to national divergences and it can therefore be more difficult to operate across European borders, since national legislation inherently varies.

An EU regulation is a legal act of the European Union that becomes directly enforceable as law in all member states simultaneously (European Commission, 2017). This helps companies to operate across EU borders, as the legislative requirements will be identical.

When the GDPR enters into effect, it replaces the previous Data Protection Directive and all local implementations thereof as the ruling piece of legislation on data privacy in the EU. This means that it is almost exactly the same across nations, with only minor differences (one of which, is the Age of Consent. The GDPR has a required Age of Consent of 16 years, but allows for member countries to adopt a Age of Consent as low as 13 years old). This standardisation allows for greater competition across EU borders and for standardisation of processes.

Definitions in the GDPR

The GDPR is more explicit than the Data Protection Directive and the Danish appropriation (Persondataloven). This can be shown multiple times throughout the legislation, for instance, if we examine the definition of what personal data is within each piece of legislation.

In the *Persondatalov*, the definition of personal data was defined as:

> *"'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject');"* - Persondataloven (2000)

But this was merely the Danish implementation of the directive, if we examine the directive directly it defined personal data as:

> *(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;* - Data Protection Directive (1995)

The directive expands further on the Danish implementation, by expanding on the definition on an identifiable person. This clarification is missing from the Danish implementation. If we look at the same definition within the GDPR:

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"* – General Data Protection Regulation, (2016)

Not only does the GDPR expand the definition within the data protection directive by specifying location data, name and online identifiers which are not specified within the directive. But it is vastly more explicit than the previous Danish implementation, that is only stating *'any information relating to an identified or identifiable natural person'* leaves ambiguity for what constitutes personal data.

Another example of the new regulation being more explicit is seen by examining the definition of consent. While all three pieces of legislation (Data Protection Directive, Personal Data Law, GDPR) has almost the same definition of consent:

> *"The data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."*- Data Protection Directive (1995) & General Data Protection Regulation (2016)

Only minor differences in formulation is found in the GDPR. However the GDPR goes on to further expand on consent, in a very explicit manner, which does not exists within previous legislation, neither the European nor the Danish appropriation.

> *"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."* – General Data Protection Regulation, (2016)

Here, the GDPR goes into great detail as to what constitutes a consent, while explicitly defining a very used practice of pre-ticked boxes to not constitute a valid consent.

Another way that the GDPR is more explicit can be found in the number of defined terms in each piece of legislation. The Data Protection Directive makes 9 definitions related to the type of data and processing in the legislation, of which the Danish Persondatalov has 8 definitions. The GDPR has 26 different definitions of types of data and processing, to further clarify the legislation.

The GDPR also introduces a few new rights for the data subject in relation to the data controllers or organisations handling their data.

Rights in the GDPR

Right of Data Portability (General Data Protection Regulation, Art. 20, 2016)
This right introduces the ability for the data subjects (individuals) to demand control over their data, and be allowed to move between different controllers or platforms. In practice this means that each data controller need to be able to export all data to their customers in a machine readable format. The Data Protection Directive included no such provision.

Identifying data subjects (General Data Protection Regulation, Art. 12, 2016)
This relates to third parties attempting to exercise a data subject's rights without proper authorisation. The Data Protection Directive does nothing to mitigate this, but the GDPR includes an article specifying data controllers must verify the identity of a data subject before giving effect to their rights, thus ensuring that data is not handed to third parties without proper consent. This is especially relevant given the large amount of API's allowing data to be shared between platforms.

Time limits for complying with the rights of data subjects (General Data Protection Regulation, Art. 12, 2016)
While the Data Protection Directive does not include any time limits for complying with requests of the data subjects directly, it does require this to be part of the national implementation of the directive. This causes different EU member countries to have different time limits for complying. Under the General Data Protection Regulation, all these time limits are controlled directly by the regulation, serving to standardise time limits across borders.

Obligation to inform data subject of the right to object (General Data Protection Regulation, Art. 13, 2016)
Under the Data Protection Directive there exists no obligation to inform data subjects of their rights. This is explicitly included in the GDPR, requiring companies to inform their users of their explicit rights; directly and at the first point of contact.

GDPR According to the Financial Institutions

We asked our interviewees regarding their opinion on the changes to the legislation as compared to previously, and if they felt that it was more explicit with regards to their handling of personal data. In this section we will also categorise the responses of our interviewees in relation to the category *'Specificity of legislation'*.

> *"The GDPR is clearly more specific than previous legislation in the area of personal data management. The current legislation has, in my opinion, not followed the digital development. So GDPR does, to a higher degree, help organisations with thinking in the right direction. But there is still a large task in interpreting and implementing the new regulation."*- Simon Frank Wendelboe, Nykredit 2018

Simon Frank Wendelboe is clearly under the impression that the GDPR is more explicit. He further expresses his feeling that the previous legislation has not kept up with the digital development. Based on this we have chosen to score Nykredits answer as a more explicit process (10)

> *"It is not easy to answer either yes or no to this [specificity of GDPR]. On the one hand there has been some new requirements for, among others, impact analysis, data portability, responsibility of data processors and more. But, at the core, the basic principles for treating personal data, and the requirement for transparency remains at the same level in relation to the data subject. It is merely the consequences of breaking the rules that has been substantially increased"* - Majken Christoffersen, Jyske Bank 2018

Majken Christoffersen states that she does feel that there are new requirements but, in the end, the basic principles have stayed the same. The most significant change is to the consequences of non-compliance. Majken Christoffersen does suggest that it is very difficult to answer this question, therefore we have chosen to classify the process as slightly complex (4)

> *"The current personal data law, already contains a large part of what the GDPR is bringing, so the difference is in the end not that large. The major difference is in the consequence of non-compliance and the increased awareness in the media as a consequence of various data leaks and challenges surrounding social media"* - Jens Klæbel, Danske Bank 2018

Jens Klæbel largely agreed with Majken Christoffersen in that the new legislation already contains most of the same requirements as the GDPR. He highlights that the major difference is in the consequences. We have scored his answer as complex (3) because of this.
He also mentions the increase in the awareness of data-subjects as a difference, suggesting this has been a factor in the decision making process.

> *"I feel that the GDPR legislation is more specific than previous. I'm thinking first and foremost on the demand that we are able to demonstrate that our processes are in compliance with the regulation.*
>
> *At the same time, it is, very clear that many may wish that there were clearer description of what is demanded of us. It is in the meantime here, that it is up to the individual organisation to determine what is necessary in relation to 'technical and organisation measures' to protect 'rights and freedom of natural persons' with a background in the organisation you are running."* - Ellen Pløger, Nordea 2018

Ellen Pløger, like Simon Frank Wendelboe, feels that the GDPR is more explicit as she highlights the requirement that they will be able to demonstrate compliance. She further elaborates that many organisations would have wished for even more clear descriptions of what is demanded of them. She states that it is up to the individual organisation to determine what is necessary to protect the rights and freedom of natural persons. As such we have chosen to score this as explicit (7).

Overall, we see that there is a general consensus that the GDPR is more explicit than the previous regulation (Simon Frank Wendelboe, Nykredit 2018; Ellen Pløger, Nordea 2018). However, there is still a lot that is up for interpretation with no clear answer on the exact requirements (Ellen Pløger, Nordea 2018; Majken Christoffersen, Jyske Bank 2018; Simon Frank Wendelboe, Nykredit 2018). To put these findings in relation to our conceptual framework, we can extrapolate that the GDPR is *more explicit*, and consequently *less specific* as a process in an outsourcing context.

Summary of the GDPR

While our interviewees are split on whether or not the legislation has become more explicit, the average score of their responses are explicit (6), and they do all agree that the legislation has introduced new demands, and a much more severe consequence of non-compliance.

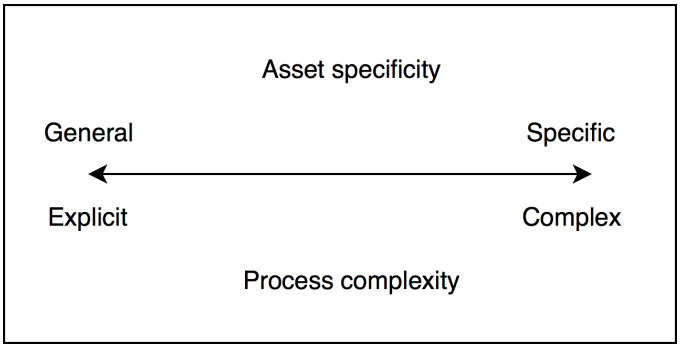


Figure 7 - Relationship between asset specificity and process complexity

The exact requirements and rights of the individuals are more explicit put in the new GDPR, than in the previous Data Protective Directive. The rights have generally also been expanded - but that does not necessarily affect the specificity of the process of being compliant, at least in the context of outsourcing Since the GDPR also standardised the personal data management regulation across European countries, then the specificity has decreased since the market has become more unified.

We would argue that because the new legislation appears much more explicit in its wording, while simultaneously introducing new rights and being unified across borders, the process of implementing personal data management solutions compliant with the new legislation have become more general (Figure 7). This has generalized the asset specificity of implementing these personal data management solutions in an outsourcing context.

The real question is then *how* much more general the process has become from an outsourcing perspective. While calculating this in any numerical value is outside the scope of this paper, we can examine how our sample organisations have acted in relation to the regulation, and make deductions about their position in our conceptual framework.

The Position of the Financial Institutions

We have now examined the GDPR closely, both through the legislation itself, its historical context, and through our interviewees. We will finish reviewing our interviewees statements regarding the categories we have created, and score each statement in relation to the categories. We will then conclude our analysis by putting both the GDPR and the financial institutions in the context of our conceptual framework.

	Danske Bank	Jyske Bank	Nordea	Nykredit
Size of undertaking	*"GDPR has been a major undertaking for Danske Bank, of that there is no question, we have invested a 3 digit million amount in compliance"*	*"(...) What you always hear from Datatilsynet and other legislative authoratives, is that if you already are compliant, then you won't have a big problem, because GDPR is only a continuation of already existing law. (...) but of course somethings with GDPR are new, and the sanctions are very different."*	*"I think it would be fair to say it has been a major undertaking, that's not to say there haven't been a lot of legislation previously, but it's apparant that GDPR increases the focus on personal data"*	*"I would say that the financial sector has had an advantage compared to the other sectors, as we are already heavily regulated. Therefore it doesn't hit us as hard as it might do to others." (...)* *"(...) this is the first regulation which affects the entire business. Most of the other regulation are department specific, so it is located with a specific group"*
Outsourced Competencies	*"We haven't outsourced anything"*	*"We haven't really outsourced competencies, we have had some external legal help (...) We have also had a consultancy help us doing a data flow analysis (...) but that's the biggest place we have had external help."*	*"We have had a lot of the competencies internally, (...) we have had some consultants to assist as arms and legs, but also for their competencies, but mostly to have some more power in the implementation phase"* *+ "I don't believe that we have made any larger IT implementations due to this [Red. GDPR]"* *+ "We are also in the process of developing a new Core Banking platform, which would have some of the elements that is required"*	*"We have decided to develop our own solution in the first round".*
Considered Outsourcing	*"We are a very large player in the market, therefore we can solve most of the problems ourselves"*	*"We have not" (discussed outsourcing)*	*"No there hasn't [been any discussion on outsourcing]"* *"Then I'll think we will hit a more general Outsourcing discussion. As in, how much does one wish to do yourself and how much does one wish to put to outsourcing. And I don't think GDPR breaks anything for us in that discussion."* *"But that also depends on the size of the company. If we take Denmark, then we see that the local banks, for good reasons, join forces. While, in some different aspects, Nordea and Danske Bank are so big that we are doing some more things ourselves, because we have the critical mass to have the competencies." - Ellen Pløger, Nordea (2018)*	

	Danske Bank	Jyske Bank	Nordea	Nykredit
Specificity of Compliance	*It is not easy to answer either yes or no to this [specificity of GDPR]. On the one hand there has been some new requirements for, among others, impact analysis, data portability, responsibility of data processors and more. But, at the core, the basic principles for treating personal data, and the requirement for transparency remains at the same level in relation to the data subject. It is merely the consequences of breaking the rules that has been substantially increased*	*It is not easy to answer either yes or no to this [specificity of GDPR]. On the one hand there has been some new requirements for, among others, impact analysis, data portability, responsibility of data processors and more. But, at the core, the basic principles for treating personal data, and the requirement for transparency remains at the same level in relation to the data subject. It is merely the consequences of breaking the rules that has been substantially increased*	*I feel that the GDPR legislation are more specific than previous. I'm thinking first and foremost on the demand that we be able to demonstrate that our processes are in compliance with the regulation.* *At the same time, it is very clear that many may wish that there were clearer description of what is demanded of us. It is in the meantime here, that it is up to the individual organisation to determine what is necessary in relation to 'technical and organisation measures' to protect 'rights and freedom of natural persons' with a background in the organisation you are running."*	*"The GDPR is clearly more specific than previous legislation in the area of personal data management. The current legislation has, in my opinion, not followed the digital development. So GDPR does, to a higher degree, help organisations with thinking in the right direction. But there is still a large task in interpreting and implementing the new regulation."*
Legal changes as a driver of change	*"We have also used GDPR as a snowplow, to clean up some things, an organisation that has Danske Banks age and size will naturally have a few messes here and there. As such we have also used GDPR as an excuse to clean up"*	*We have solutions in place to be, generally, compliant [on the 25th of May]. But I am not completely satisfied with our solutions as is. I know that we have had to chose to use many manuel processes (...) where, eventually, we would like to implement system processes. However, because it is expensive and extensive to make those system changes, and it is not completely known exactly how broad it would become. I mean, if there are 3 persons who would like to use their data-portability during the course of a year, then it is not cost effective to create a solution that costs multiple 100.000 DKK."*	*"I believe that when new legislation arrives, you always review old processes, and sometimes you find some things that needs to be changed (...) so it is obvious that the increased awareness from GDPR results in actions, also on the technical side"*	*"GPDR has increased our awareness of the management of customer data" (H)* *"Many has been surprised, it used to be like the Wild West" (H)* *"One of the good things about GDPR[in releation to as a driver of change], is that is personally relationable. It is yours and my data that is circulated, and how would I feel, if someone were just passing my personal information around on e-mail to 10 or 20 persons? So clearly it has changed peoples attitude to personal data." (S)* *"Are we looking a bit broader, on a group level, then I think it has help push us towards a development that many is in (...) and that is that Data is Gold."*

Table 3 - Interviewee statements

Size of Undertaking

As previously mentioned, this category is meant to categorise how each organisation felt about the task of becoming compliant with the GDPR, from a minor to major and with a numerical scale from 0-10.

Danske Bank

> *"GDPR has been a major undertaking for Danske Bank, of that there is no question, we have invested a 3 digit million amount in compliance"* - Jens Klæbel, Danske Bank (2018)

Danske Bank clearly believes that the GDPR has been a major undertaking, even going so far as to state '*there is no question'* about it. Jens Klæbel highlights the amount of resources they have spent on compliance. He further states that this was done in an effort to automate a lot of the process, specifically regarding the right to data portability (Jens Klæbel, Danske Bank 2018). We have scored Danske Bank as a 9 and a major undertaking.

Nykredit

> *"There is still a large task in interpreting and implementing the new regulation."*- Simon Frank Wendelboe, Nykredit 2018

Nykredit suggests that it is a large task to interpret and implement solutions to the GDPR, however as mentioned later:

> *"I would say that the financial sector has had an advantage compared to the other sectors, as we are already heavily regulated. Therefore, it doesn't hit us as hard as it might do to others (...) this is the first regulation which affects the entire business. Most of the other regulation are department specific, so it is located with a specific group"* - Simon Frank Wendelboe, Nykredit (2018)

Simon Frank Wendelboe believes that the GDPR has generally been a large task, but also suggest that there have been some mitigating factors for the banking industry since it is already heavily regulated, as opposed to other industries. Simon Frank Wendelboe also highlights that this is the first regulation that affect the entire business. Because of this we have decided to score Nykredit as a major undertaking, but given them a smaller score of 7 to represent some of their supposedly mitigating circumstances.

Jyske Bank

> *"What you always hear from Datatilsynet, and other legislative authorities, is that if you already are compliant, then you won't have a big problem, because GDPR is only a continuation of already existing law (...) but of course some things with GDPR are new, and the sanctions are very different."* - Sjanna Evers Spliid, Jyske Bank (2018)

Sjanna Evers Spliid, suggests that there are some new aspects of the legislation, but generally that if you are already compliant with the personal data law, then the challenge of GDPR is not too extensive. We have chosen to score Jyske Bank as a major undertaking with a score of 6, which is only slightly categorised as major. This is done because they do suggest some new aspects of GDPR and highlights the increased sanctions, but they are relatively close to indifference between classifying it as a major or minor undertaking. Please note that classifying the undertaking as a 5, would not mean that it is a small undertaking, that would be a lower score such as 1, it would simply mean that they do not see it as a major undertaking.

Nordea

> *"I think it would be fair to say it has been a major undertaking. That's not to say there haven't been a lot of legislation previously, but it's apparent that GDPR increases the focus on personal data"* - Ellen Pløger, Nordea (2018)

Nordea highlights that it is a major undertaking. But they also mention that there has been legislation in the same area. We have chosen to score Nordea as major (8). Not quite as firm a position as Danske Bank but they still believe that it is a major undertaking.

Generally, it appears that all organisations tend towards the GDPR as being a major undertaking. The average score is 7,5. Most of the interviewees mention that there has been some new requirements introduced from the GDPR, but that many of the requirements are similar to those that the financial sector is already exposed to. It is also suggested that the banking industry are more geared towards regulatory compliance compared to other industries, since they are already under heavy regulation. Finally, Nykredit suggests that this is the first piece of legislation that is prevalent throughout every corner of their organisation, as opposed to previous legislation.

Outsourced Competencies

This category relates to whether or not the organisations actually chose to outsource their competencies or develop solutions and processes in-house.

Nordea

> *"We have had a lot of the competencies internally, (...) we have had some consultants to assist as 'arms and legs', but also for their competencies, but mostly to have some more power in the implementation phase"*- Ellen Pløger, Nordea (2018)

> *"I don't believe that we have made any larger IT implementations due to this [GDPR]"*
> - Ellen Pløger, Nordea (2018)

> *"We are also in the process of developing a new Core Banking platform, which would have some of the elements that is required"* - Ellen Pløger, Nordea (2018)

Nordea argued that they have not outsourced any process per se, but they have hired in additional *'arms and legs'* both for their pure work manpower but also for their additional competencies. Specifically, they argue that they have not made any large IT implementations due to GDPR. But this was also due to the fact that they are developing a new *Core Banking* platform, which would have many of the capabilities required of GDPR. That platform is currently being tested in Finland and will be rolled out to the rest of Nordea once completely finished. We can therefore conclude that Nordea has chosen to mainly keep the competencies in-house, and we have therefore chosen to score Nordea as a no (7), they have not outsourced anything, but have chosen to get a little bit of outside help.

Jyske Bank

> *"We haven't really outsourced competencies, we have had some external legal help (...) We have also had a consultancy help us doing a data flow analysis (...) but that's the biggest place we have had external help."* - Sjanna Evers Spliid, Jyske Bank (2018)

Jyske Bank, similarly to Nordea have not outsourced anything but chosen to hire small help in the form of consultants, and not considered outsourcing. We have chosen to score them similarly to Nordea with a no (7).

Danske Bank

> *"We haven't outsourced anything"* - Jens Klæbel, Danske Bank (2018)

Danske Bank was very firm in their statement, categorically denying any outsourcing. We have scored them with no (10).

Nykredit

> *"We have decided to develop our own solution in the first round".* - Simon Frank Wendelboe, Nykredit (2018)

Nykredit also denied any outsourcing, but still kept the possibility open in the future. Thus not as categorical denial as Danske Bank, and was scored with no (9).

All organisations chose to not outsource in relation to GDPR, the average score was no (8,25). While some organisations did acquire some external help in developing their solutions, it was very clearly in-house solutions across all organisations.

Considered Outsourcing

As all organisations chose not to outsource, we naturally followed up the question with asking if they had considered outsourcing. This category relates to these questions.

Nordea

> *"No there hasn't [been any discussion on outsourcing]"* - Ellen Pløger, Nordea (2018)

Nordea states that they have not had any discussion about whether or not to outsource, they further state that:

> *"But that [outsourcing] also depends on the size of the company. If we take Denmark, then we see that the local banks, for good reasons, join forces. While, in some different aspects, Nordea and Danske Bank are so big that we are doing some more things ourselves, because we have the critical mass to have the competencies."* - Ellen Pløger, Nordea (2018)

Here, Ellen Pløger suggests that the size of the bank has an influence on outsourcing and that larger banks have the capabilities to develop systems and processes internally, while smaller local banks '*join forces*'.

> *"Then I'll think we will hit a more general outsourcing discussion. As in, how much does one wish to do yourself and how much does one wish to put to outsourcing. And I don't think GDPR breaks or changes anything for us in that discussion."* - Ellen Pløger, Nordea (2018)

Ellen Pløger then further reiterates that the GDPR have had no impact on the outsourcing discussion at Nordea.

> *"The fundamental idea has been to not invent anything new unless absolutely necessary, instead we would rather update what we have"* - Ellen Pløger, Nordea (2018)

It is clear from these statements, that Nordea has not considered outsourcing at all. Ellen Pløger directly states that Nordea has not considered outsourcing personal data management and she elaborates on that position through a few points. The first one being that she believes that outsourcing any process depends largely on the size of the organisation. In her opinion, outsourcing of personal data management might be of interest to smaller banks in the Danish banking sector, but for large players, such as Danske Bank and Nordea, it is not the case. Furthermore, Ellen Pløger does not believe that GDPR in and of itself has changed anything regarding to their perspective on outsourcing. This may also help to explain why Nordea has not considered using outsourcing to solve, at least part of, the challenges associated with the GDPR. This is also building on what Ellen Pløger mentioned in her previous response, that they are building a new Core Banking platform. From her, and Nordea's, point of view, it would not make sense to build or purchase anything new, unless it was absolutely necessary since they are in the process of building it anyway. We have scored Nordea as a no (10) because they made it very clear that they did not discuss outsourcing, and had no intention of considering it.

Danske Bank

> *"We are a very large player in the market, therefore we can solve most of the problems ourselves"* - Jens Klæbel, Danske Bank (2018)

Danske Bank also states that they have made no considerations towards outsourcing, which reflects the position from Ellen Pløger (Nordea, 2018), where they both agree that their respective company is large

enough, that it does not need to outsource their personal data management due to the GDPR. Danske Bank was scored with a no (10).

Nykredit

> *"Due to the size of Nykredit, we have the competences internally to drive GDPR forward. Therefore, there has not been any discussion of external outsourcing. As an institutions we are used to navigate in an area that are heavily regulated. In this sense the GDPR are only a small part of our regulatory landscape"* - Simon Frank Wendelboe, Nykredit (2018)

The position of Nykredit is very similar to Danske Bank and Nordea, in that they have the size to develop these solutions themselves, and therefore did not discuss the possibility of outsourcing. They further state that they are used to dealing with compliance because of the industri they are in. We have scored Nykredit as a no (10) as with the other organisation, because they did not give any indication of the slightest discussion of the subject.

The overall consensus was very clear in this category, with an average score of no (10), no organisations considered outsourcing even the slightest. Mostly stating their size as the reason, and the fact that the banking industry is so heavily regulated already.

Legal Changes as a Driver of Change

An additional thing we uncovered during our interviews, was that some organisation used the implementation of GDPR to facilitate other changes within the organisations. We chose to include these findings for both discussion and future research possibilities.

Danske Bank

> *"We have also used GDPR as a snowplow, to clean up some things, an organisation that has Danske Banks age and size will naturally have a few messes here and there. As such we have also used GDPR as an excuse to clean up"* - Jens Klæbel, Danske Bank (2018)

It is clear that Danske Bank has used GDPR as an excuse to clean up internal processes. Interestingly, that might have an effect on the outsourcing case. If Danske Bank could achieve some internal scale advantages then that might have made the internal clean-up a more efficient venture, at least when comparing it relative

to outsourcing. We have chosen to score this as a yes (9) because it was clearly suggested that they had used to GDPR as an excuse to facilitate a secondary process.

Nykredit

> *"One of the good things about GDPR [in relation to GDPR as a driver of change], is that it is personally relatable. It is yours and my data that is circulated (...) So clearly it has changed people's attitude to personal data."* - Simon Frank Wendelboe, Nykredit (2018)

> *"Are we looking a bit broader, on a group level, then I think it has help push us towards a development that many* [companies] *are in (...) and that is that data is gold."* - Simon Frank Wendelboe, Nykredit (2018)

Nykredit has also used GDPR as an excuse to clean up their business processes. It has helped motivate individuals in the organisation to put a higher emphasis on personal data which has made changes easier to complete - all in favour of keeping processes in-house. Furthermore, GDPR has helped Nykredit to realise that *"data is gold"* which can be classified as a higher level decision. But the realisation that *"data is gold"* implies a higher focus on IT being Core Competencies, which according to the outsourcing literature (Straub et. al, 2008) does not promote outsourcing. We have chosen to score them as a Yes (9).

Nordea

> *"I believe that when new legislation arrives, you always review old processes, and sometimes you find some things that needs to be changed (...) so it is obvious that the increased awareness results in actions, also on the technical side"* - Ellen Pløger, Nordea (2018)

Ellen Pløger from Nordea also believes that the increased awareness caused by the GDPR has resulted in actions, implied clean-up actions both on the business process side, but also on the technical side, thus we chosen to score them as a yes (7).

Jyske Bank

> *We have solutions in place to be, generally, compliant [on the 25th of May]. But I am not completely satisfied with our solutions as it is. I know that have chosen to use many manual processes (...) where, eventually, we would like to implement system processes. However, because it is expensive*

and extensive to make those system changes, and it is not completely known exactly how broad it would become. I mean, if there are 3 people who would like to use their data-portability during the course of a year, then it is not cost effective to create a solution that costs multiple 100.000 DKK. - Sjanna Evers Spliid, Jyske Bank (2018).

We see here that Jyske Bank is a bit different than the others. They have not chosen to use GDPR as an excuse to clean up their processes in general. But have rather made sure that they will be compliant with the legislation, and then use the eventual outcome to determine whether they should increase their effort within GDPR compliance. This is the reason we have chosen to categorize Jyske Bank as a no (4), since they will rather wait and see, instead of using it as an excuse to "*clean up*".

We see more mixed results in this category, some organisations have clearly used the GDPR as a way to either perform cleanup or facilitate other secondary processes related to data within the respective organisations. While other organisations have not used to GDPR as anything other than a new legislation to be implemented. The overall average score in this category was yes (7,25).

Summary

	Danske Bank	Jyske Bank	Nordea	Nykredit	Average
Size of undertaking	Major (9)	Major (6)	Major (8)	Major (7)	Major (7,5)
Outsourced competencies	No (10)	No (7)	No (7)	No (9)	No (8,25)
Considered outsourcing	No (10)	-	No (10)	No (10)	No (10)
Specificity of compliance	Complex (3)	Complex (4)	Explicit (7)	Explicit (10)	Explicit (6)
Legal changes as a driver of change	Yes (9)	No (4)	Yes (7)	Yes (9)	Yes (7,25)

Table 4 - Summary of categorisation

It is clear that all the financial institutions we have interviewed, have seen GDPR as a major undertaking. The degree to which has varied a bit, but generally it has been a major undertaking. While it was a major

undertaking, we also see that all of our case companies has chosen to keep competencies in-house, specifically with regards to personal data management. The banks have used consultants, sector advisor groups (such as Finans Danmark), and the authorities to gauge the best way to be compliant with the new GDPR. Furthermore, consultants have been used to some extent, to clarify internal data processes.

Interestingly, we see that the banks generally have not even considered outsourcing, with pretty high confidence. Lastly, the banks have generally seen the GDPR as a way to prioritise general clean-up of internal processes. The exception here is Jyske Bank, which is taking a more cautious approach. While Jyske Bank expects to be fully compliant by the implementation deadline, they are more cautious about implementing huge changes for what could possibly be a small customer demand.

Results

Now we have looked at the General Data Protection Regulation, we have put the legislation in a historical context and looked at the changes from the Data Protection Directive. We have also asked our interviewees about their position regarding the legislation and we have additionally examined how they have dealt with the legislation. In this section we will put this in the context of our conceptual framework. We will discuss each point in the framework in relation to our results and findings. We will then finish the section by summarising our findings. But first we will reintroduce the conceptual framework that were introduced previously.

1. The specificity of an asset, process or product can be increased or decreased by legislation.
2. Decreasing the specificity of a process should result in:
    a. An increase in the difference in production costs ΔC
    b. An increase in the difference in governance costs ΔG
3. An increase in ΔC + ΔG to a point above Â (Figure 8), should result in an increase of market procurement for that process

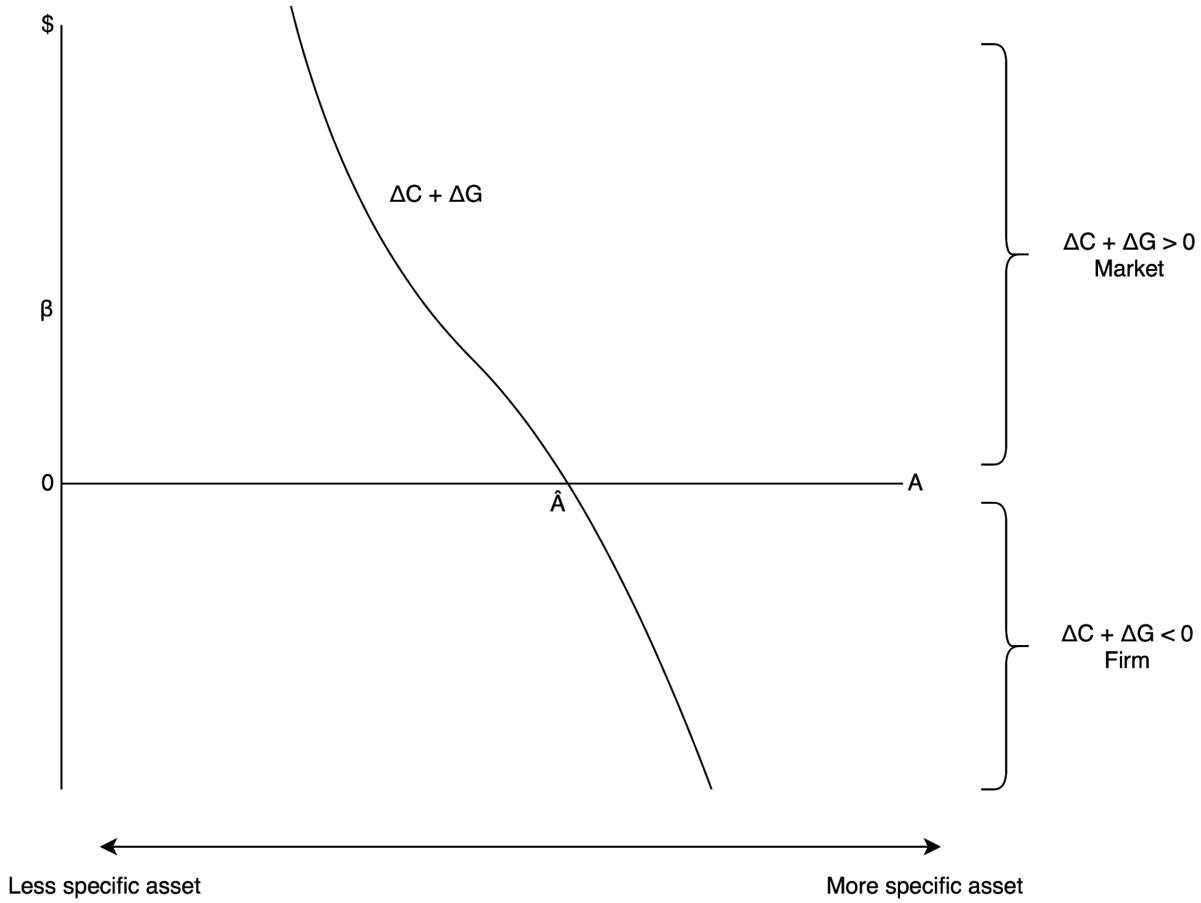


Figure 8 - Conceptual Framework Model

When discussing (1) the specificity of an asset, we previously defined three types of asset specificity.

- Site specificity, which is related to the geographical position of the good or investment,
- Physical asset specificity, which is related to equipment and tools, and
- Human asset specificity, which is human knowledge, learning and skills.

Site specificity

The first type of asset specificity is the site specificity. Traditionally, site specificity has referred to geographical located of e.g. natural resources. While this has little consequences here, a different type of geographical site specificity might be. If we view legislation as the specific component in personal data management, then the variances in each national implementation of the Data Protection Directive (Figure 9) will increase specificity since such a process would need to account for the differences in national legislation. If legislation were to be standardised across national borders, as the GDPR does, then it could decrease the site specificity for solutions involving personal data management since a single implementation does not need to account for differences in the legislation between countries.

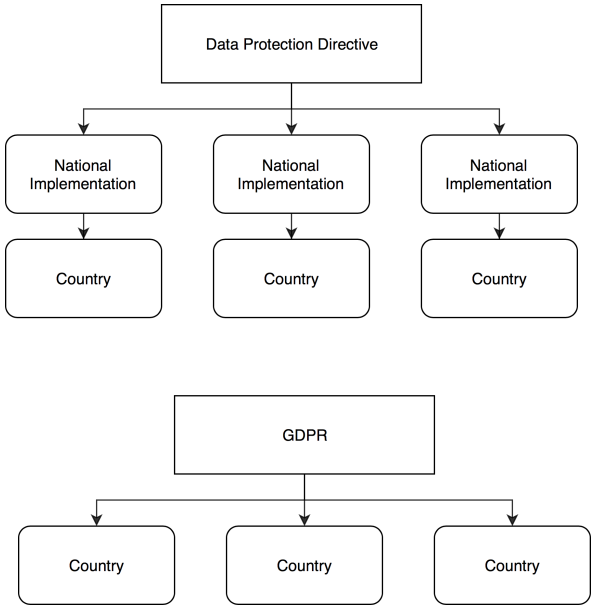


Figure 9 - Data Protection Directive and GDPR

We argue that because the GDPR spans across borders as a single piece of legislation, the site specificity of complying with the legislation has decreased slightly.

Physical asset specificity

When discussing the systems or processes that will help organisations become compliant with the GDPR, we are discussing physical asset specificity.

As we see through our review of the GDPR, the demands faced by firms imposed by the new regulation are more well defined and explicit than previously. We saw this both in our analysis of the legislation, where the phrasing of the legislation was more explicit and the number of definitions was increased substantially. We saw it somewhat in our interviews with the financial institutions where the category *specificity of compliance*

scored a 6, being viewed as slightly more specific. We argue that both of these facts serves to decrease the physical asset specificity of being compliant with the regulation.

But the GDPR also include new provisions that were previously not something firms had to comply with, as we saw through our analysis of the regulation. This was also confirmed through our interviews with the financial institutions, who generally felt that *size of undertaking* was major, scoring a 7,5 in this category. It was also mentioned by several of the organisations that both the new implementations and the consequences of non-compliance were contributing factors (Ellen Pløger, Nordea 2018; Jens Klæbel, Danske Bank 2018). We argue that this has been an increased burden on the organisations, as they have to be compliant with more regulation than previously. However, it has not directly affected the physical asset specificity of the GDPR.

We therefore argue that the overall physical asset specificity has been decreased, mainly because of the more explicit nature of the GDPR even though it contains more provisions than previously.

Human asset specificity

We did not find conclusive evidence of changes to human asset specificity, and generally changes to learning and human knowledge will most likely be more apparent after the legislation has gone into effect. However, we did find some organisations mentioning internal training of employees in a quite broad context throughout the organisations (Ellen Pløger, Nordea 2018). This could suggest an increase in human asset specificity, as certain new knowledge, and more specialised employees are required. This argument can be further substantiated by the fact that the GDPR requires organisations to have a dedicated Data Protection Officer, which is the title held by some of our interviewees. A job with highly specialised knowledge in the data practices within the firm. However, this training will have to be done

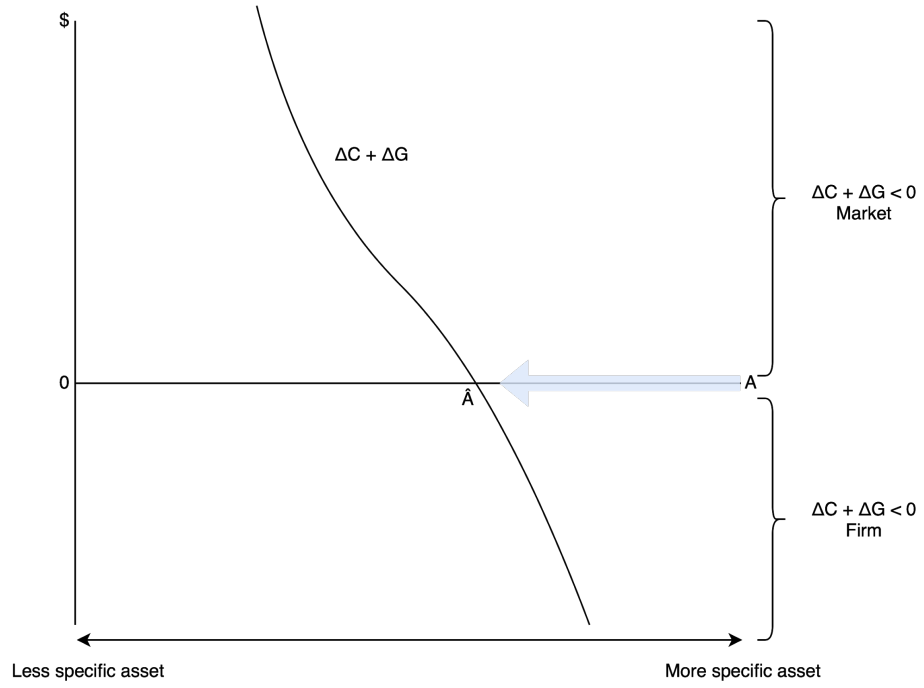


Figure 10 - Theorised change to asset specificity

regardless of the process of personal data management is being outsourced or not. So the potential increase in human asset specificity could be argued to have no or very limited effect on the level of specificity.

Given this, we argue that the overall specificity of the asset can change given changes in legislation. As an effect of the decrease to *site specificity* and *physical asset specificity*, we argue that these decreases outweigh the potential negligible increase in *human asset specificity*, which would result in an overall decrease in asset specificity. This would cause the effect illustrated in Figure 10, that the general asset specificity has decreased.

In our conceptual framework, we see that a decrease in asset specificity, should lead to an increase in the production costs differences between the market and the firm, increasing the advantage of the market over the firm. We would also expect to see an increase in the governance costs difference, tending towards an advantage for the market. It is important to highlight that these are tendencies and not absolute values.

We see that decreasing the specificity of a process or product should increase both the difference in production costs ΔC and the difference in governance costs ΔG.
For GDPR, we generally see that the cost of being compliant with regulation has increased substantially (Khan, 2017). A quick reasoning would therefore be that the specificity of compliance with legislation has increase, as evidenced in the increased costs. However, that is potentially a misleading correlation. Costs have risen, there seems to be little doubt about this, as we see in the category *Size of Undertaking* which was scored as a major undertaking 7,5. But likewise the task of being compliant has also grown. A larger process does not necessarily mean that it is a more specific task - when viewing it from a outsourcing perspective. Instead, it might actually have decreased the specificity of the task of personal data management, since all industries now have been more aligned in what can and cannot be done to personal data. Before GDPR, personal data was managed very differently, depending on the company and the sector of which it operated. Now, the personal data management might be more aligned across industries, which would create a larger market for a potential third party provider. As seen in the Transaction Cost Economics literature, we know that the size of the potential market correlates with the potential for the market to have a higher production cost difference (ΔC) in contrast to internal production, primarily due to economies of scale advantages.

Whether the GDPR has caused an actual decrease in specificity of personal data management is difficult to measure precisely. This is partly due to the nature of personal data management, that it is difficult to define the exact requirements that is necessary for personal data management and for GDPR compliance in general. One of the reason is the degree to which each bank has chosen to define what should be done to be compliant (Ellen Pløger, Nordea 2018). Some banks have chosen to make everything automatic, while others might

only digitize what makes sense from a business point of view. Therefore, limiting the personal data management area to a precise area that is easily measurable is difficult with such an broad area. Different banks might have different definitions on what exactly constitutes *personal data management*, which naturally would affect how accurate potential numbers could be, even if we had access to them.

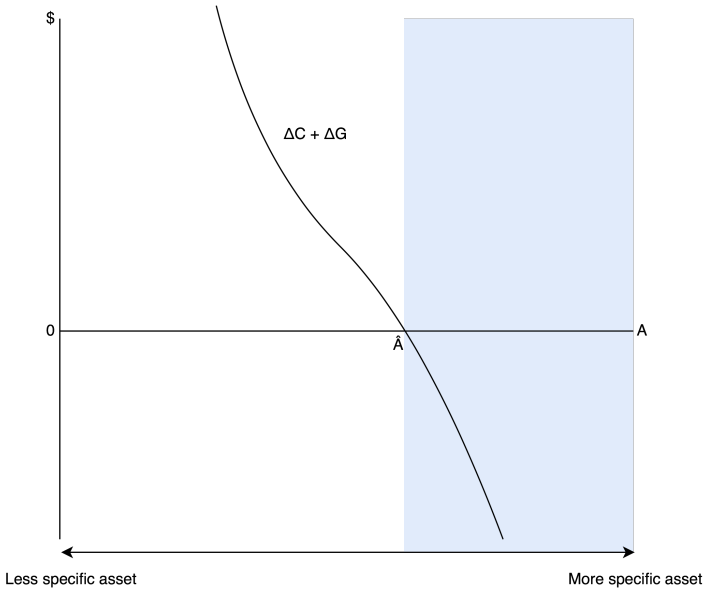


Figure 11 - Section of internal production

To sum up, the decrease of an asset's or process' specificity, should increase the differences in production cost (ΔC) and governance costs (ΔG) between internal production and external procurement. This decrease can potentially lead to outsourcing.

As we just saw in the previous section, there are evidence that the decrease in asset specificity should increase the differences in production costs (ΔC) and governance costs (ΔG) to the market's advantage. This increase can collectively be described as ΔC + ΔG. However, evidenced by our interview, we saw that no organisations have chosen to outsource any part of the GDPR. If we try to relate this to our conceptual framework from earlier(Figure 11), then we can extrapolate the following; If all our participants choose *not* to outsource then, by the inherent logic of the framework, all of our case companies considered the process of personal data management to be in the blue zone, as depicted in Figure 11. Total costs ΔC + ΔG is thus lower internally than externally.

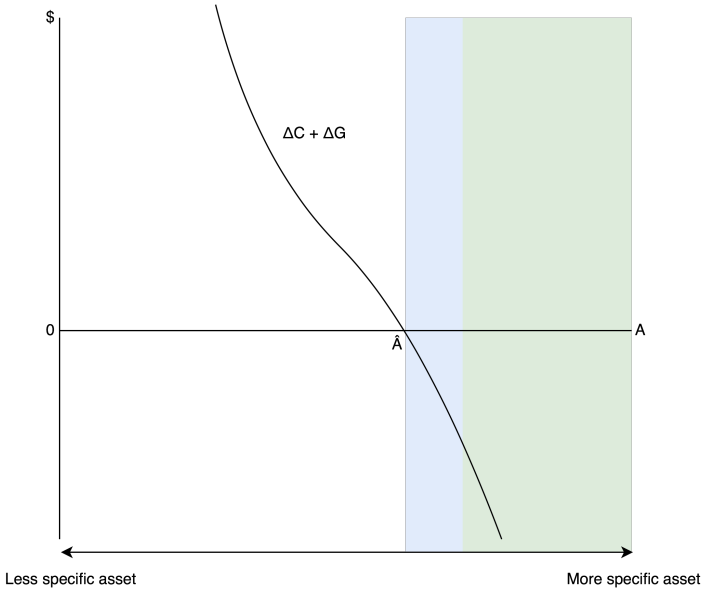


Figure 12 - Point of no consideration

Even with the lack of actual data and numbers, we can make further logical deductions. Since we have seen that none of the interviewed organisations have even considered outsourcing, then they must logically be some distance from the point of indifference (Â). Given bounded rationality it logically follows that organisations close to the point of indifference would consider outsourcing as a viable option. However, since none of the financial institutions even considered outsourcing, the they would be located even further to the right, as illustrated by the green area in Figure 12.

Uncertainty & Frequency

As previously discussed uncertainty can be relevant for outsourcing. From the result of our interviewees' expressing a lack of clarification regarding the implementation of compliance processes, we argue that uncertainty has increased, as can be seen in the following quote from Ellen Pløger from Nordea.

> *"At the same time, it is very clear that many may wish that there were clearer description of what is demanded of us. It is in the meantime here, that it is up to the individual organisation to determine what is necessary in relation to 'technical and organisation measures' to protect 'rights and freedom of natural persons' with a background in the organisation you are running."* - Ellen Pløger, Nordea 2018

As the asset in focus is compliance with legislation, organisations will gain no benefit from being 'overly' compliant. Thus all organisations theoretically strive to only invest just enough to be compliant with the legislation. We argue that this results in an increased uncertainty due to a lack of information of how much to invest.

Another point affecting uncertainty can be seen if we examine the right to data portability. This is one of the new rights introduced with the GDPR. And this legislation has brought with it a 'demand' side of the legislation, since data-subjects can actually demand their data in a machine readable format.

The organisations implementation of this right has been very different, some have been very automated as seen by Danske Bank, who have automated the process so that the data subjects can request and receive their data with almost no delay (Jens Klæbel, Danske Bank 2018). While others have to a greater extent been much more manual (Simon Frank Wendelboe, Nykredit, 2018; Ellen Pløger, Nordea, 2018).

All organisations however expressed an uncertainty towards how much the data subjects would use this right, whether it would be a monthly/quarterly thing or simply a one-time thing some people will test out

when the legislation enters into effect (Simon Frank Wendelboe, Nykredit, 2018; Sjanna Evers Spliid, Jyske Bank, 2018).

While manual processes have a lower fixed cost, they are only cost efficient when the quantity is low. On the other hand, automated processes are relatively expensive to set up, but scales very efficiently with increased demand. Consequently, the imperfect level of information, regarding the volume of certain aspects of GDPR, generally increases the level of uncertainty.

Another point we found, was that the increased awareness from the public on data handling and privacy had increased the awareness of the organisations on the same topics. And the organisations was very aware that they could be 'embarrassed' publicly if they were found to not be compliant. This could also attribute to uncertainty relating to outsourcing, since even though they outsourced personal data management to a third party, the 'blame' or 'embarrassment' of a failure would still fall on them, this was mentioned directly by Ellen Pløger (Nordea, 2018).

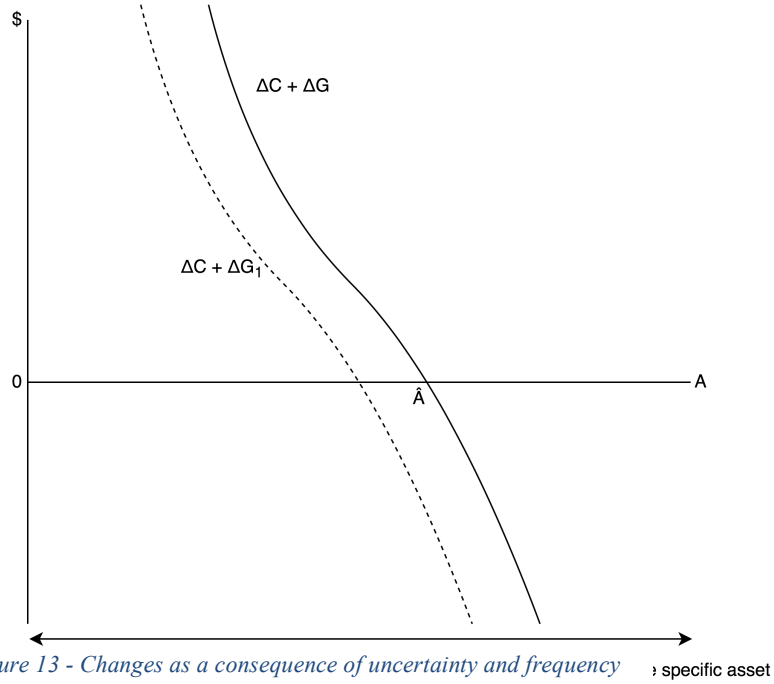


Figure 13 - Changes as a consequence of uncertainty and frequency

As defined earlier, the third property affecting transactions, apart from specificity and uncertainty is frequency. Williamson described this property as the least significant of the three. We argue that frequency has little to no impact, since building processes for compliance would only need to be implemented as legislation changes, and this would be negligible in the decision process.

We argue that the overall uncertainty has increased, which will result in line $\Delta C + \Delta G$ shifting to the left as $\Delta C + \Delta G_1$. So if the asset specificity is actually at the point of indifference, but the costs $\Delta C + \Delta G$ has shifted to $\Delta C + \Delta G_1$ then we see that internal production is still favourable – even if the asset specificity does not solely account for the underlying reason. This relationship is depicted in Figure 13.

To end our analysis, we will summarize our findings. If we look at our conceptual framework again:

1. The specificity of an asset, process or product can be increased or decreased by legislation.
2. Decreasing the specificity of a process should result in:
    a. An increase in the difference in production costs ΔC
    b. An increase in the difference in governance costs ΔG
3. An increase in ΔC + ΔG to a point above Â, should result in an increase of market procurement for that process

(1) We have seen that the specificity of an asset, in this case compliance with the GDPR and personal data management, has decreased. This is observed directly from looking at the legislation and from the responses in our interviews. We examined the three sub areas, *Site specificity*, *physical asset specificity* and *human asset specificity* and collectively we saw that the specificity decreased - even though the task of compliance might be larger.

(2) In the second part of our conceptual framework, we see that an increase in the potential market for third party providers should, by the effects of economies of scale, increase the difference in production costs advantage for the market.
Similarly, the explicit nature of the GDPR should also help to standardise the personal data management processes across organisations and industries. By having more standardised product descriptions, it should be easier, and thereby less expensive, to govern the production of personal data management. Less expensive and simpler governance should increase the potential for market procurement.

(3) From the onset of this thesis, we expected to see some organisation outsource their personal data management as described in our conceptual framework. However, as we have seen throughout this analysis we have found no evidence of outsourcing. Furthermore, we have found no evidence of any of our organisations even considering outsourcing as a viable option. We can infer several implications as a result of this, which we will go into detail about in the following section.

Discussion

Throughout this section, we will discuss some of the implications of this study, both in relation to practical implications and the theoretical implications of the findings in this paper.
We will discuss the timing of this paper in relation to the findings, we will briefly examine the supply side of personal data management and we will discuss the regulatory changes in relation to change as a whole and not just outsourcing which was a bi-product of our interviews. We will then move on to discuss some of the limitations of the methodology in this study, the limitations of our findings and our approach. We will end this section by framing these discussions in relation to future research, and what areas that advantageously could be explored further.

Theoretical Implications

Non Significant Results

From the onset of this thesis, we expected to see some organisation outsource their personal data management. However, that has not been the case.

There are three possible, logical deductions as to why we do not see the expected results.

1. The asset specificity has simply not moved ΔC + ΔG to a point beyond Â,
2. Uncertainty limits the effects, or
3. Inconclusive nature of TCE in relation to IT outsourcing

The first logical deduction is that decreased specificity of the new GDPR has simply not moved to a point beyond Â. Our empirical data shows no evidence of large, Danish financial institutions outsourcing due to GDPR. This can be due to either that the asset specificity, A, has not moved enough to go beyond the point of indifference, Â, or it simply did not move at all. If we look at Figure 14, then we see that when specificity

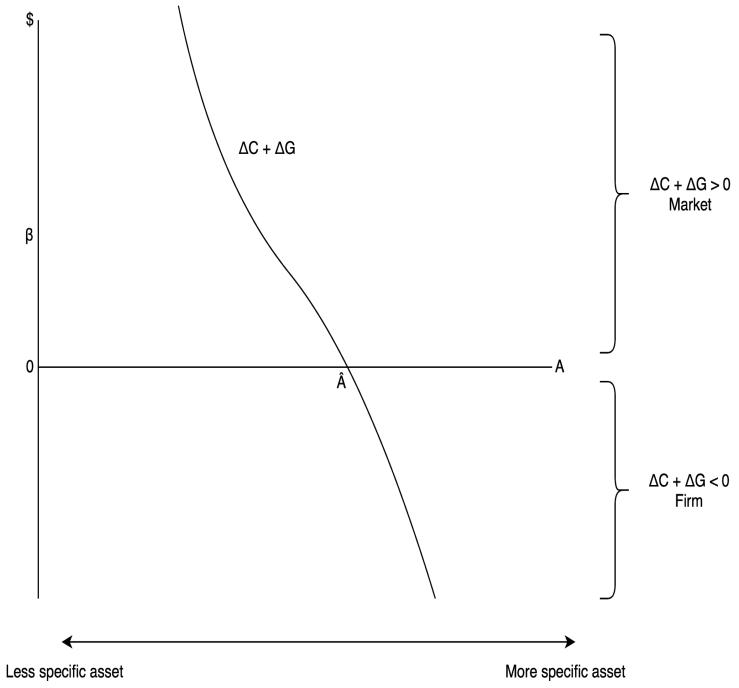


Figure 14 - Conceptual Framework Model

decreases, then we will find a intersect point on ΔC + ΔG. Organisations should only outsource when ΔC + ΔG > 0, so a logical conclusion would be that this is still not the case. This does not mean that the specificity has not decreased, but it merely means that it has not decreased enough. However, it might also mean that there has been no movement of the specificity at all, or even that the specificity has increased. With the data that we have collected, we cannot confidently conclude or exclude any of these points. However, we will argue that the most likely of these three options (decreased specificity, no change or increased specificity) is that the specificity has decreased, just not enough.

The second logical deduction is that we see no effects on outsourcing, primarily due to increased uncertainty and bounded rationale. The GDPR and personal data management is a complex area and is hard to precisely define and confine. What one company might define as personal data management, might not be included for a different company. The internal IT systems might also influence how easy it is to separate different processes. This influenced the uncertainty aspect which would mean that uncertainty shifts the whole ΔC + ΔG to the left, which would make any given specificity more likely to be internally produced as seen in Figure 13. There is a high degree of uncertainty associated with GDPR, which might also influence the financial organisations to be less willing to commit to outsourcing of personal data management.

The last possibly deduction is in the inherent problems with TCE. As we previously described in our literary review, we saw mixed results concerning the validity of the theory. However, we did also see that it was the theory most frequently used to study the IT outsourcing phenomenon (Lacity et. al. 2011). Lacity et. al. (2011) studied the validity of TCE in relation to IT outsourcing, and found four possibly determinants of why we observe such mixed results.
Two of these determinants could be relevant in explaining our results, with the first being the measurement problem. This relates to the difficulties in defining and measuring the TCE construct. Our study, of outsourcing as a consequence of GDPR, has been broadly examining the GDPR as a whole. It is possible that this has introduced a measurement problem due to the broad nature of compliance with the GDPR. It can be difficult to separate what constitutes exclusively personal data management and what is a part of the broader GDPR compliance. The second relevant determinant has to do with boundary conditions, and relates to the fact that the TCE theory is being used to study a phenomenon outside of the scope for which TCE was originally intended. This is also a feasible reason why our results are inconsistent with the theory, simply because we have used TCE to study IT outsourcing related to regulations for which is was not originally designed.

We believe that the answer lies between the first and second deduction. That asset specificity has indeed become less specific and that uncertainty has increased. These two conditions combined, can explain why we see no outsourcing from the financial institutions.

Legal Changes as a Driver of Change

One thing, that we did not initially set out to analyse, but was discovered throughout our interactions with the different organisations, is that some organisations has used this legislation as a way of doing '*cleanup'* or maintenance internally in the organisations processes and IT systems. It was neatly summarized by Jens Klæbel from Danske Bank.

> *"We have also used GDPR as a snowplow, to clean up some things, an organisation that has Danske Banks age and size will naturally have a few messes here and there. As such we have also used GDPR as an excuse to clean up"* - Jens Klæbel, Danske Bank (2018)

The other organisations response can also be read in the section *the Position of the Financial Institutions*, but a general consensus was that the banks have used the implementation of GDPR to combine a lot of cleanup, that was eventually due, and take the cost at the same time as the GDPR implementation.

Practical implications

Complexity of Personal Data Management

A possibility is that within the market of larger financial institutions, the process of outsourcing personal data management is simply too complex and fundamental to be outsourced. We saw that the organisations we interviewed recognised the rising importance of data (Simon Frank Wendelboe, Nykredit 2018; Jens Klæbel, Danske Bank 2018), and perhaps this change towards a data-driven mindset is causing the data management aspects of financial institutions to become core competencies. An attributing factor to this could also be the increased public awareness surrounding data privacy, which the organisations also recognised (Ellen Pløger, Nordea 2018; Jens Klæbel, Danske Bank 2018). As our literary review suggested, core competencies should not be outsourced, and it is a possibility that data management within large financial institutions are moving towards being a core competency.

Supply & Demand

This thesis has primarily focused on the demand side of outsourcing the personal data management processes. However, there are always two sides to a case, and in economics there are the demand and the supply side. If there is no supply side, then it does not matter how large the demand side is. For this area it would mean that if there is no providers that offer a simple, cheap and effective solution that efficiently handles the whole personal data management area, then that might explain why we see no outsourcing in the financial industry. One could further argue, that since GDPR only goes into effect on the 25th of May, 2018, which is after the publication of this thesis, then we have still not seen the full potential of the market yet. Since the market is partly being created by the GDPR, then the effects of economies of scale might not be observable yet. The economies of scale argument is the primary reason why markets are more efficient than the firm (Williamson, 1981). One could suppose that the personal data market is still in its infancy, which might explain why there is such a low drive for outsourcing.

If we take a quick look at the supply side of the personal data management market, then we see that the FinTech and RegTech market is booming. Frost & Sullivan (2017) estimates that the global RegTech sector will have a Compounded Annual Growth Rate (CAGR) of 76,1% by 2020, reaching a total value of 40 billion DKK. Many new companies are being created in the field of personal data management, in the following table we have comprised a few:

Company	Solution
NewBanking	A platform solution that verifies and stores personal data and allows individuals to share and manage their personal information.
Norbloc	Focuses on removing duplication of effort by reusing data. End-user is in full control of their personal information.
Trunomi	Enabling end-users to share their data with full consent. High focus on user consent.
Trulioo	Focuses on verifying individuals. Highly specialised in verification of individuals, albeit with no consumer-facing services.

Table 5 - Emerging suppliers of personal data management

Many more can be found, but here we only provide a small view of the companies that are arising within personal data management. We also expect more to arise once GDPR goes into effect.

If this was indeed the main cause why we do not see outsourcing, then we could, with reasonable confidence, expect to see large financial institutions at least consider outsourcing. But during our interviews, we saw no evidence of the large, Danish financial institution even considering outsourcing. One potential cause of this,

could be that the decision makers have a relatively good understanding of the services that is available and therefore do not even consider what they, reasonable, might believe to be non-existing. Therefore, we might not see managerial awareness of potential solutions until they are more widespread.

Limitations

In the following section we will discuss some of the limitations this study, and how they relate to the results we found. We will attempt to reflect critically on our work, so as to provide the reader with as clear a picture as possible of the work in question.

One of the limitations of any qualitative study, is that the qualitative nature makes it very difficult to make precise conclusions aside from tendencies. We can make observations on the asset specificity, uncertainty and frequency based on our analysis and argue the implications based on what we find.

This is limited to our selected data. Since we have only investigated larger financial institutions, it could be that this is very different for other private organisations to manage, especially if personal data is not central to their business and they are not as used to handling compliance as these financial institutions which all mentioned were very heavily regulated already (Ellen Pløger, Nordea 2018; Jens Klæbel, Danske Bank 2018; Simon Frank Wendelboe, Nykredit 2018). It could also be very different for smaller banks. We observed several of the organisations we interviewed mentioning that, because of their size, they were better equipped to handle the GDPR as opposed to some of the smaller banks (Ellen Pløger, Nordea 2018; Jens Klæbel, Danske Bank 2018). From our initial research, when analysing the different markets, we learned that most smaller banks in Denmark all outsource IT systems to just a few suppliers. It could be interesting to see how the IT suppliers have handled the GDPR implementation and compare that to the larger institutions. However, the suppliers we reached out to refused to participate in our study.

It is also limited since we cannot define more precisely what value $\Delta C + \Delta G$ is. In our analysis it is not possible to put definitive numerical values on these, which limits us to make observations about tendencies. To achieve a greater understanding of the organisations in relation to our conceptual framework beyond tendencies, we would need to define compliance much more detailed. It is generally agreed, both from our analysis and our interviews that the new legislation is more specific. However, we have no way to measure to what extent. Furthermore, we have no way to define and compare the production costs and governance costs between our organisations because the data is very hard to come by. A clear definition of how such costs should be calculated has not been within the scope of this paper.

An issue there may have been relating to our research methodology, is in the definition of the outsourcing concept towards our interviewees. We experienced some resistance during some of the interviews when asking about outsourcing. We should probably have defined the outsourcing concept for each interviewee at the onset of the interviews, as to leave no confusion or individual interpretation about what we considered to be outsourcing.

Another point related to our conceptual framework, which we also will go into more detail with in the future research section of this paper, is the time horizon of this study. As this study is a cross-sectional study (Saunders, 2012) the focus has been on a *'snapshot'* in time, i.e. we studied if the organisations have outsourced at this particular point in time. It could be the case, that the market for personal data management simply have not matured enough yet. As of this paper, the GDPR have not yet entered into effect and there are still quite a few areas that are open to interpretation. Once we see the requirements stabilize a bit, and potentially a decrease in the relevant uncertainty aspect, we might see companies begin to provide personal data management solutions. One of the areas we directly saw uncertainty from our interviewees was at the scope of how often data subjects would utilise their rights, e.g. *'The Right to Data Portability'* (Ellen Pløger, Nordea, 2018; Sjanna Evers Spliid, Jyske Bank, 2018). And creating specialised systems or acquiring these systems through outsourcing, may not be economically feasible (Sjanna Evers Spliid, Jyske Bank, 2018).

Future Research

One area that could be expended upon in future research, is looking at different markets or industries. We have come to learn that the financial sector is already subject to a lot of legislative requirements (Jens Klæbel, Danske Bank 2018; Simon Frank Wendelboe, Nykredit 2018). Instead of potentially outsourcing some of it, we see that they feel that they already have the relevant competencies in-house to be compliant. However, that may not be identical for other industries. A potential future research area could therefore be to see if our findings are similar across other industries. The results might be different for industries that are not so heavily regulated.

Another area for future research is the emergent field of personal data management. As we briefly touched upon, we saw a tendency for an increasing market for personal data management in the upcoming FinTech and RegTech industry. So it could be interesting to see how the market has evolved in a few years, after the GDPR has become common practice and when the potentials of the market, such as economies of scale, have had time to go into effect. We would expect to see a lot more companies considering and actually using such a solution, once it becomes accepted in the market. There might also be a tendency for companies to take a cautious approach when outsourcing regulatory compliance, as the consequences can be quite substantial,

e.g. the GDPR has potential fines of 4% of global, annual turnover, not to mention the brand damages that can arise as well.

An interesting point that could be examined through further research, is a more precise examination of the legislation. In this study we have made a cursory examination of the legislation as a whole, and examined the tendencies and the impact of the legislation. But an interesting point could be to go a step further and make a quantitative study of a more specific part of the legislation. This could for example be how companies have implemented the right to data portability. By defining the research area to a more specific part of the legislation, the phenomenon can be studied even further. It would be simpler to examine the costs associated with a specific aspect of the GDPR more directly and with a larger data sample than the one within this paper.

Conclusion

The goal of this thesis was to answer the following research question:

To what extent has the decreased specificity of the General Data Protection Regulation promoted outsourcing of personal data management in large financial institutions?

This was done through a careful examination of relevant literature and through that the development of a conceptual framework with which the examination of the research question could occur.

Through our conceptual framework, we demonstrated that the GDPR has indeed made some aspects of legislative compliance more explicit. This increased level of explicitness has translated into a higher degree of generalisation of the processes. This is observed directly from looking at the legislation and from the responses in our interviews.

It has become apparent that none of the largest financial institutions in Denmark have actually outsourced anything significant due to the GDPR. The supposed effect of the increased explicitness of the processes has not been sufficient for financials institutions to consider outsourcing personal data management. They have relied on consultancies for information on various items, such as the expected legislative consequences and to facilitate various workshops and personal data flow mappings. But none of them have used any outsourcing company or system to outsource personal data management.

Since none of the organisations we interviewed had chosen to outsource, and given the explanatory nature of this study, we investigated further to whether or not they had considered outsourcing, and what considerations that went into their decision. There was a clear consensus amongst the organisations that they had not considered outsourcing in any way.

As previously discussed, there can be three possible reasons as to why we do not observe any outsourcing, given the decreased asset specificity of the GDPR.

1. The asset specificity has not moved to a point beyond the point of indifference (Â)
   Based on our category *Specificity of Compliance* and our analysis of the GDPR, we can deduct that a possibility is that the asset specificity has indeed moved, but not enough to push ΔC + ΔG beyond Â.

2. Uncertainty limits the effects
   The increased uncertainty we observed in relation to the regulation has limited the effects of the changes to the outsourcing decision.

3. Inconclusive nature of TCE in relation to IT outsourcing
   The third option is that we have encountered what Lacity et al. (2011) described as either the measurement problem or boundary conditions which has limited our analysis.

We argue that the results can be explained by a combination of the first and second deduction. That asset specificity has indeed become less specific and that uncertainty has increased. These two conditions combined, can explain why we see no outsourcing from the financial institutions.

The findings in this paper are conclusive, given the analysis in this thesis, we feel confident in concluding that the General Data Protection Regulation has to no or very limited extent promoted personal data management outsourcing in larger financial institutions.

References

Alaghehband, F. K, Sazanne Rivard, Shikui Wu, Sylvain Goyette (2011), 'An assessment of the use of transaction cost theory in information technology outsourcing', Journal of Strategic Information Systems

Badshah, N. (2018, April 08). Facebook to contact 87 million users affected by data breach. Retrieved from https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach

Blind, Knut (2011), *'The influence of regulations on innovation: A quantitative assessment for OECD countries*', Elsevier (2011), doi:10.1016/j.respol.2011.08.008.

Butterworth, T. (2018, March 26). Europe is doing way more than the US to protect online privacy. Retrieved from https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge

Carter, R. and Hodgson, G. M. (2006) '*The Impact of Emperical Tests of Transaction Cost Economics on the Debate on the Nature of the Firm*', Strategic Management Journal, Strat. Mgmt. J., 27: 461–476 (2006), DOI: 10.1002/smj.531

Currie, W., 1998. Using multiple suppliers to mitigate the risk of IT outsourcing at ICI and Wessex Water. Journal of Information Technology 13.

Currie, W., Willcocks, L., 1998. Analyzing four types of IT sourcing decisions in the context of scale, client/supplier interdependency and risk mitigation.

Coase, R. H. (1937). The Nature of the Firm (Vol. 4, Ser. 16). The London School of Economics and Political Science: Economica.

Data Protection Directive (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union.
Link: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A31995L0046&from=EN

European Commission (2017, October 24). Regulations, Directives and other acts - European Union - European Commission. Retrieved from https://europa.eu/european-union/eu-law/legal-acts_en

Frost & Sullivan (2017), *RegTech in Financial Services*, Global, Forecast to 2020. Report MCB0-33

General Data Protection Regulation, (2016), '*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).'*, Official Journal of the European Union.
Link: http://eur-lex.europa.eu/eli/reg/2016/679/oj

Global outsourcing market size 2017 | Statistic. Retrieved from https://www.statista.com/statistics/189788/global-outsourcing-market-size/

Gonzalez, R.. J. Gasco. J. Llopis Information Systems Outsourcing reasons and risks: a new assessment 2010

Kvale, S. (2007). Doing Interviews. Los Angeles: SAGE Publications.

Khan, M. (2017, November 19). Companies face high cost to meet new EU data protection rules. Retrieved from https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc

Klæbel, J (2018). Personal Interview

Lacity, M., Willcocks, L., 2000. Survey of IT outsourcing experiences in US and UK organizations. Journal of Global Information Management.

Lacity M, Stan Solomon, Aihua Yan, Leslie, P Willcocks (2011) 'Business Process Outsourcing studies: a critical review and research directions', Journal of Information Technology, DOI: 0268-3962/11

Lacity, M, Leslie P. Willcocks and Shaji Khan (2011), '*Beyond Transaction Cost Economics: Towards an endogenous theory of Information Technology Outsourcing*', Journal of Strategic Information Systems 20 (2011) 139–157.

Levina, N., Ross, J., 2003. From the vendor's perspective: exploring the value proposition in information technology outsourcing. MIS Quarterly.

Loebbecke, C., Huyskens, C., 2006. What drives netsourcing decisions? An empirical analysis. European Journal of Information Systems 15.

The Nobel Foundation, '*Oliver E. Williamson - Facts'*. (2009). Retrieved from https://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2009/williamson-facts.html

Persondataloven (2000), *Lov nr 429 af 31/05/2000*, Pubslished in '*Lovtidende*' A. Link: https://www.retsinformation.dk/forms/r0710.aspx?id=828

Pløger, E (2018). Personal Interview

Robert J. David and Shin-Kap Han (2004) '*A Systematic Assessment of The Empirical Support For Transaction Cost Economics*', Wiler Interscience, DOI: 10.1002/smj.359

Saunders, Carol & Gebelt, Mary & Hu, Qing. (1997). Achieving Success in Information Systems Outsourcing. California Management Review. 39. 63-79. 10.2307/41165887.

Saunders, M. N., Lewis, P., & Thornhill, A. (2016). Research methods for business students. Harlow, Essex, England: Pearson Education Limited.

Seddon, P.B., 2001. The Australian federal government's clustered-agency IT outsourcing experiment. Communications of the AIS 5

Straub, D., Weill, P., Schwaig, K., 2008. Strategic dependence on the IT resource and outsourcing: a test of the strategic control model. Information Systems

Spliid, E. S (2018). Personal Interview

Teng, J., Cheon, M., Grover, V., 1995. Decisions to outsource information systems functions: testing a strategy-theoretic discrepancy model. Decision

TheBanks.eu. (2016). Largest Banks In Europe. Retrieved from https://thebanks.eu/top-banks-by-assets

Vaxevanou, A. and Konstantopoulos, N. (2015) '*Models Referring to Outsourcing Theory*', Procedia - Social and Behavioral Sciences. Elsevier B.V., 175, pp. 572–578. doi: 10.1016/j.sbspro.2015.01.1239.

Venkatraman, L, N., 1992. Determinants of information technology outsourcing: a cross-sectional analysis. Journal of Management Information

Wendelboe, S. F,. Andersen, R, H (2018). Personal Interview

Williamson, O.E., (1979). Transaction-cost economics: the governance of contractual relations. Journal of Law and Economics 22 (2)

Williamson, O. E. (1981). *The economics of organization: The transaction cost approach*. S.l.: S.n.

Williamson, O.E., 1985. *The Economics Institutions of Capitalism: Firms, Markets, Relational Contracting*. Free Press, New York.

Williamson, O. E. (2010). The mechanisms of governance. New York: Oxford Univ. Press.

List of Appendices

FINANSTILSYNET

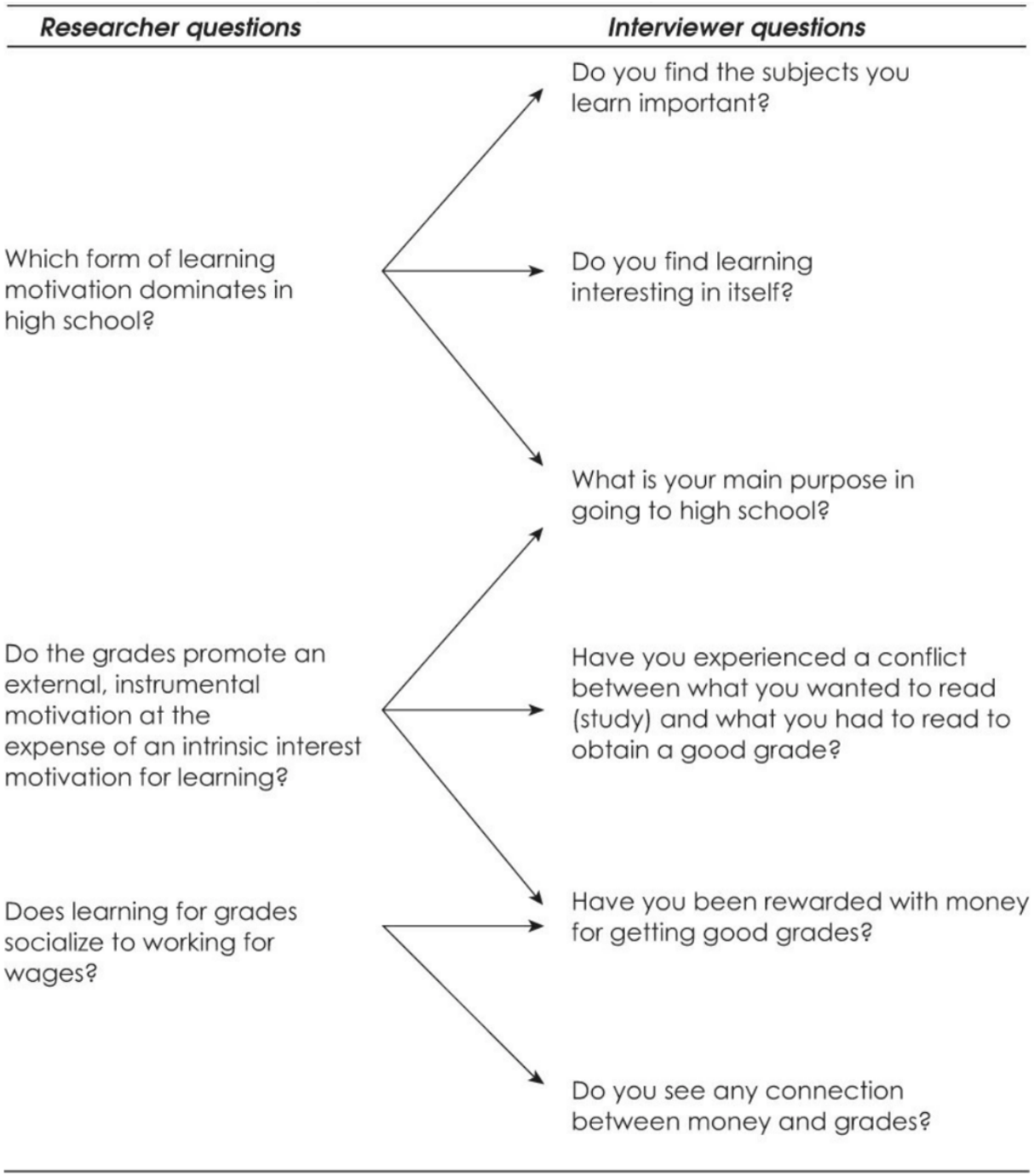
Pengeinstitutternes størrelsesgruppering 2016

Gruppe 1 - Arb. kapital over 75 mia. kr.	
3000	Danske Bank A/S
2222	Nordea Bank Danmark A/S
7858	Jyske Bank A/S
8079	Sydbank A/S
8117	Nykredit Bank A/S

Gruppe 2 - Arb. kapital over 12 mia. kr.	
9380	Spar Nord Bank A/S
5301	Arbejdernes Landsbank, Aktieselskab
1149	Saxo Bank A/S
7730	Vestjysk Bank A/S
7670	Ringkjøbing Landbobank, Aktieselskab
8099	Nordjyske Bank A/S
9335	Kronjylland, Sparekassen
9686	Den Jyske Sparekasse
400	Lån og Spar Bank A/S
9217	Jutlander Bank A/S
522	Sjælland, Sparekassen
9070	Sparekassen Vendsyssel

Gruppe 3 - Arb. kapital over 500 mio. kr.	
7681	Alm. Brand Bank A/S
5999	Danske Andelskassers Bank A/S
10001	FIH Erhvervsbank A/S
755	Middelfart Sparekasse
6771	Lægernes Pensionsbank A/S
7320	Djurslands Bank A/S
9090	Sparekassen Thy
9740	Frøs Herreds Sparekasse
844	Fynske Bank A/S
828	Sparekassen Fyn A/S
7780	Skjern Bank, Aktieselskabet
6471	Grønlandsbanken, Aktieselskab
9695	Saxo Privatbank A/S
7230	Østjydsk Bank A/S
7890	Salling Bank A/S
6520	Lollands Bank, Aktieselskab
13460	Merkur, Den Almennyttige Andelskasse
7930	Kreditbanken A/S
6860	Nordfyns Bank Aktieselskabet

Appendix 2 - Steinar Kvale (Doing Interviews) Research questions and interview questions



Interviewguide

Introduction

- Who are we?
- Why this study?
- What is the expected outcome?

Personal information

- Position/title & department
    - Position within bank
    - Working title
    - Level of involvement with GDPR
- Experience & history with bank

GDPR compliant

- How has your organisation reacted to GDPR?
- What steps has been taken to be compliant with GDPR
- Do you expect that your organisation will have completed implemented the final solution to GDPR before the implementation deadline?
- Did your firm have the capabilities to be compliant internally?
- Has this process been a minor undertaking or a larger undertaking for your firm?
- Have you updated old processes to be compliant or developed new ones?
- Have any processes or capabilities been outsourced in order to be compliant?
- Has the other banks approach to GDPR compliance influenced your decision?
- How did the opinion of the FSA (Financial Service Authorities / “Finanstilsynet”) influence your decision?

Appendix 4 - Jyske Bank Interview

Participants:

Carsten Svaneborg (C)
Andreas Hald (A)
Sjanna Evers Spliid (S)
Majken Christoffersen (M)

Who:	What:
A	Vil du ikke starte med at fortælle lidt om dig og hvad du laver i Jyske Bank?
S	Jo. I september blev jeg DPO (Data Protection Officer) i Jyske Bank. Som fuldstændig er bundet op på de her principper der er i forordningen (Red. persondataforordningen) i den stilling. Og det har vi valgt i Jyske Bank. Og det er jo en frivillig beslutning. Der er jo ikke nogen der har sagt at banker de skal have en DPO. Det har sådan ligget lidt i kortene, og man kan jo se, nu ved jeg ikke hvor meget i har dvælet ved artikel 29-gruppens udtalelse eller sådan hvor meget I har gravet i det juridiske..?
C	Vi har ikke været inde og se deres udtalelser endnu.
S	Men hvis altså at man sådan graver lidt i (??) og artikel 29-gruppens, som er den gruppe der på Europæisk plan sidder og laver vejledninger. Det er sammenslutning af repræsentanter fra den Europæiske datatilsyn. Så kan man se at de sådan skriver.. Eller indikere at forsikringsselskaber og organisationer der behandler store mængder af data og laver kreditscoringer og den slags ting, de formengentligt skal have en DPO. Og ud fra den betragtning, og jeg tror faktisk også at justitsministeriet i et eller andet, mere eller mindre officielt møde havde udtalt at man måtte forvente at banker måtte have en DPO. Ud fra den betragtning, og selvfølgelig gennemgang af de juridiske krav der ligger, der er 3-4 kriterier der siger hvornår man er forpligtet til at have en DPO, det er sådan noget med omfang og kriterierne for de persondata man behandler. Der er det anbefalet at have en frivillig DPO. Det er så det vi har udnævnt i Jyske Bank med mig.
C	Er du så den eneste DPO i Jyske Bank?

S	Ja jeg er den eneste DPO som sådan i Jyske Bank. Men så har vi jo et datterselskab på Gibraltar der er der faktisk også en DPO. Men jeg er den eneste DPO på koncernniveau i Jyske Bank.
A	Er du tidligere fra Jyske Bank eller kommer du udefra Jyske Bank?
S	Jeg blev ansat 1. maj som compliance officer, med ansvaret for persondata. Og har en juridisk baggrund og kommer fra en compliance baggrund også i en helt anden branche, i møbel/tekstil branchen. Så jeg er ny i den finansielle sektor, men jeg har været vant til at arbejde med lovgivningsstof.
A	Det lyder som om vi har fået fat på den helt rigtige.
S	Det må vi se om jeg kan svare på jeres spørgsmål.
A	Hvis du skulle sætte lidt generelle ord på hvordan I, som Jyske Bank, har reageret på GDPR. Hvad ville du så sige?
S	Vi startede tilbage i efteråret '16, hvor der blev nedsat en programgruppe og et projekt. Og hvor der også blev nedsat en styregruppe. Så i efteråret 2016 var der en programgruppe og styregruppe der startede dette projekt. Og så er der så blevet koblet en mængde mere kvalificeret personer til projektet undervejs. Jeg syntes egentligt vi har behandlet det meget seriøst fra dag 1, og jeg syntes at vi gik i gang i okay tid. Det er det man altid får at vide når man er sammen med datatilsynet og andre myndigheder, at hvis man overholder de eksisterende persondatalovgivning, så har man et meget lille problem fordi man reelt set er en videreførelse af en eksisterende lov eller eksisterende regelsæt. Men der er selvfølgelig nogle ting der er fremmed og så er der selvfølgelig det lille tvist med at sanktionerne er nogle helt andre end de tidligere har været. Og man kan sige at det som er trigger der er at det tidligere har været en bøde på 25.000 og i dag taler vi jo 4% af årlig omsætning, hvilket vil være et 3-cifret millionbeløb for Jyske Bank. Så det gør jo lidt ift. prioriteringen af sådan et projekt i en virksomhed. Og jeg tror det er helt på linje med andres håndtering eller approach. Eller det kan jeg jo konstatere, for der har ikke rigtigt været nogen konsekvens ved ikke at leve op til de persondatalovgivningen hidtil.
A	Ja for mange virksomheder har det jo været en cost-benefit analyse, hvis det er billigere

	at tage bøden end at få styr på det så…
S	Ja 100%. Og man kommer heller ikke langt med et IT projekt eller systemændringer for 25.000.
Alle	Griner sammen.
S	Ikke dermed sagt at man ikke skal være compliant med lovgivningen, men man må også se i øjnene at i sådan nogle organisationer som Jyske Bank og lignende, så er der bare en mængde lovgivning man skal være compliant med. Og der tager man jo fra en kant af og starter der en risikobaseret tilgang, og der er persondataloven bare ikke ligget højt på prioriteringslisten.
A	Nu her, er det ikke d. 25 maj den træder i kraft? ville du sige at i var compliant på det tidspunkt? så vidt jeg ved så har datatilsynet udtalt at de ikke vil slå hårdt ned i starten, og i stedet starte med nogle advarsler. Er i klar fra dag et?, eller bliver det en 'ongoing' process
S	Det bliver helt klart en ongoing process, altså vi har en løsning på plads på de væsentligste områder, altså ud fra en risikobaseret tilgang, og også forsigtighedsprincip. Og så har vi løsninger på plads til at være, sådan, overvejende compliant. Men jeg er ikke tilfreds med løsningerne som sådan, vi har måtte vælge at tilgå med mange manuelle processer f.eks ved (mumler...) hvor man på sigt gerne ville implementere systemløsninger, men fordi det er dyrt og omfangsgribende at lave de systemændringer, og man heller ikke helt ved, hvor vildt bliver det? altså er der 3 i løbet af et år der vil have dataportabilitet? Så kan det måske ikke betale sig at lave en løsning der koster flere 100.000.
	(interviewet bliver kort afbrudt af barn i baggrunden)
S	Ja, man er jo ligesom nødsaget til på en eller anden måde lige at se hvad for et monster det er. Noget som f.eks dataportabilitet eller indsigtsret men man kan jo sagtens være compliant ved at lave håndholdte løsninger.
A	Ja bestemt.
S	Det er der jo ikke noget problem i, men dermed er det jo ikke sagt at det ikke kunne være fedt at lave f.eks løsninger i netbanken så de bare lige kunne trykke på en knap og

	sige “hent mine data” eller “giv mig indsigt i hvad i har på mig”
A	Ja, en af de andre banker vi har haft snakket med, var bl.a. meget bange for specielt journalister. og hvad de kunne finde på. F.eks umiddelbart efter at lovgivningen er trådt i kraft sende e-mails med persondata rundt i organisation og så bede om at få data udleveret dagen efter.
S	Ja, det vil der jo også komme. man kan jo sagtens forestille sig undersøgelser hvor de måler bankerne op imod hinanden. “Her kan du få det” og “her giver de dig kun det” altså.. Det vil der komme et element af, det er helt sikkert. specielt hvis der er stor fokus på det i nyhederne.
C	Ja selvfølgelig det hjælper jo altid
S	Men altså, stadigvæk det er svært at sige, får man 10 henvendelser på indsigtsret i de 3 første måneder, eller får man 100. Det er jo egentligt ikke kun kunder, det er også kunde emner. f.eks kunder der har bedt om tilbud, eller ophørte kunder, som man jo bevarer i x antal år efter de har valgt at sige farvel til banken. fordi vi har nogle forpligtelser i forhold til hvidvaskningslov. Så det er en meget bred gruppe af registererede. og selvfølgelig vil der være nogle af dem som bliver irriteret på banken, eller føler de er blevet uretfærdigt behandlet. og så føler man at man kan straffe dem lidt.
A	Ja så kan man slå igen
S	Ja, det vil der jo selvfølgelig være, og så journalisterne og så sølvpapirs hattene.
Alle	griner
S	som bare generelt er bange for hvad det store net gør ved os.
A	Hvis vi dykker lidt dybere ned i de kompetencer det har krævet, nu nævnte du selv at det var en delvist manuel process i har implementeret på nogle af de her ting. Er det nogle kompetencer i har haft internt i Jyske Bank, eller er det noget i har haft brug for konsulenter til? eller måske anvendt en ekstern løsning?
S	Altså vi har ikke som sådan haft konsulenter inden ovre, vi har haft nogle forskellige advokatfirmaer til at hjælpe os når vores egen juridiske afdeling har følt at her skal vi ligesom have noget hjælp eller.

A	Et ekstra input
S	Ja et ekstra input, så har vi haft et par advokatselskaber til at hjælpe med del leverancer i forhold til det juridiske af det. og så har vi haft et konsulentfirma inde til at hjælpe os med at lave en datastrøms analyse. Vi har lavet datastrøms analyse, og det syntes jeg faktisk også var en relativt seriøs tilgang, vi lavede datastrømsanalyse her i 17, allerede tilbage fra marts og frem til september havde vi et forløb hvor vi gennemgik godt og vel 500 processer i koncernen. og der havde vi en ekstern konsulent inde og hjælpe os med at gennemføre den her datastrømsanalyse. Så det er det største område vi har haft ekstern bistand på.
C	Okay, øhm yes. Har i så generelt opdateret jeres eksisterende interne processer eller har i mere udviklede nye processer til at erstatte gamle.
S	Det kommer an på om du mener processer som forretningsgange eller systemprocesser.
C	Egentligt begge, men lad os starte med forretningsgange
S	Ja der har vi jo selvfølgelig, og er igang med nu at lave ændrede forretningsgange.
	(Kort afbrydelse af barn)
S	Forretningsgange er vi jo ved at opdatere, der er jo simpelthen nogle andre måder - hvis en kunde begynder at spørge om indsigt så må første linje af kunderådgivere ikke røre ved det, så skal vores kompetencecenter tage sig af det. Så det skal der jo nye forretningsprocesser på.
S	Der er en mængde nye politikker, også en persondata politik, som er en udvidelse af noget vi har, meget af det har vi noget af, men meget af det er også nyudviklet. Det er sådan en kombination af noget nyt og noget vi har noget af. Hvis du ser på politikker og forretningsgange
S	Og lidt det samme ved systemer.
A	En videreudvikling?
S	Ja, selvfølgelig er der nogle nye løsninger indenfor, men det er ligesom nogle afarter af noget eksisterende. Det eneste vi sådan rigtigt er ude og købe ind, er et system som kan

	sende data portabilitet ud til registrerede der ikke er kunder. og som vi derfor ikke har adgang til i vores netbanks system. Fordi dette kan E-boks ikke. Og du kan ikke bruge mail for det er en usikker forsendelsesmetode. Så der er vi ude og købe en ekstern løsning. Men det er ikke mange eksterne løsninger vi har været ude og købe. Når man f.eks taler rolle styring, der var vi allerede igang med noget som egentligt bare lå og ventede på at vi skulle bygge videre på det. Og det samme med Office 365, det havde vi også liggende og det gav også en masse i forhold til at styre hvad folk har liggende i deres mailbokse- så det var vi også igang med i forvejen, så vi har ikke som sådan været ude og lave storindkøb i forhold til det her.
A	Øhm, noget vi har hørt hos de andre banker vi har interviewet, er at de har søgt meget andre banker og bl.a. datatilsynets mening om disse reguleringer. med henblik på at finde 'normen'. Er det noget i har gjort?
S	Ja, men vi indgår jo i nogle samarbejder helt naturligt med andre banker. Vi har et sektor samarbejde i det der hedder finans danmark. Som er den her sammenslutning hvor man prøver at bistå sektoren med f.eks lovgivningen, og der er nedsat en arbejdsgruppe der sidder med GDPR. Og der er flere banker repræsenteret og der drøfter man i plenum, hvad gør i og hvad gør vi. hvordan ser det her ud og hvad er finans danmarks holdning. Skal vi have fået noget afklaring i forhold til hvidvask loven. Skal vi kontakte data tilsynet i fællesskab så vi kan ligge os på et eller andet niveau som tilsynet godkender. Så der er ligesom forskellige samarbejder. Og derudover er der også noget der hedder LOPI som er lokale pengeinstittutter, som har en styregruppe. og dem har vi også været i dialog med, selvom vi er lidt større end den generelle spiller i klassen. Og derudover indgår vi også i nogle samarbejder med nogle data centraler bank data siger det jer noget?
C	Øh, ja altså bank data siger os ikke så meget, er det ligesom SDC og BEC.
S	Ja, lige præcis
C	Ja så kender vi dem godt.
S	Ja der sidder typisk også en del banker sammen omkring en systemmæssig løsning og netbank løsninger og sådan noget. Og der er det jo helt klart at sådan noget som dette selvfølgelig også bliver diskuteret. For man skal træffe en beslutning om hvordan vil vi løfte det her systemmæssigt på vores data central. Så der har vi jo selvfølgelig også haft nogle samarbejder. og der er også noget der hedder JN data, som også er en data

	central eller leverer IT hardware, eller mere server kapacitet hvor vi også er sammen med nogle andre banker, nykredit og forskellige finansielle enheder.
C	Ja for man skal jo sørge for at hele sin linje for brugeren hele vejen ned til hvor data ligger er compliant
S	Ja for det er klart at fordi vi ikke er alene om disse løsninger så er det et samarbejde med disse aktører, og så opstår der jo helt naturligt en drøftelse om hvordan griber i de her ting an, hvordan har vi tænkt os at gribe dem an. når der nu ikke er kommet nogen officiel vejledning om en tilgang i de finansielle sektor.
S (fortsat)	Men det mangler vi jo altså. Nogle der, et eller andet sted, har taget nogle beslutnigner eller lagt op til nogle retningslinjer for de finansielle sektor. Fordi det er jo lidt specielt. Det mangler i hvert fald helt vildt. Det er også en af de ting jeg har påpeget i rapporteringen herinde før jeg går på barsel at der mangler sektor vejledning - helt vildt. Det er jo klart at de kigger jo også rundt i Europa og der er ingen andre der har lavet noget vejledningen, og så sidder de jo ligesom på deres hænder.
C	Så de gør lidt det samme som I gør (kigger rundt) bare på et højere Europæisk niveau.
S	Ja. Og så er det klart at når man er i de her samarbejder, så prøver man jo lidt at hvis vi nu alle sammen vælger den her tilgang, så vil det måske være svært for Datatilsynet at sige at 'Det er bare fuldstændig forkert', hvis der nu er en stor gruppe der har valgt at sige at det er sådan vi løser den opgave. Det er jo heller ikke sådan at Datatilsynet, hvis man lige skriver til dem, at de bare kommer tilbage og siger "vi syntes I skal løse jeres oplysningspligt sådan og sådan". Det får man jo ikke..
A	De har jo nærmest interesse i ikke at gøre det så tydeligt som muligt
S	Ja for de skal jo kontrollere det bagefter. Ja, så vi har rigtigt meget samarbejde med andre sektorer.
C	Jeg tror nogenlunde at det var de spørgsmål vi har… Og jeg tror vi har været meget godt rundt om det. Er der noget du føler kunne være relevant for os at vide? I forbindelse med GDPR og hvordan I har valgt at løse det
S	Det sidste spørgsmål undre mig lidt. 'How does the opinion of the FSA influence your

	decision'. Jeg tænkte Opinion.. Hvad er det for en opinion? Der har ikke rigtigt været nogle ude og sige noget som helst.
C	Ja netop. Så det er hvordan ville retningslinjer fra dem have en indflydelse på jeres beslutning de processer eller systemer I har valgt at bruge. Om de har anbefalet noget eller hvordan fremgangsmåde med det.
S	Der må man jo sige at de (Finanstilsynet) har været meget tilbageholdende og ikke kommet med noget vi kan bruge til noget helt konkret. Og det der også står lidt hen i det uvisse det er jo hvorvidt finanstilsynet der har tænkt sig at være tilsynsmyndighed ift. bankerne eller om det skal være datatilsynet. Det ved jeg ikke om I har hørt, men det har jo lidt været oppe og vende om det er finanstilsynet der skal ud og føre tilsyn ift. databeskyttelsereglerne.
A	Men det er ikke blevet besluttet endnu?
S	Nej
C	Nej, men der er jo også hele 2 måneder til endnu
Alle	Spredt latter
A	Ved du om det har været diskuteret højere oppe om man skulle kigge på eksterne styringsløsninger i Jyske Bank?
S	Det vil jeg ikke kunne udtale mig om med sikkerhed.
S	Ja men ved du hvad, de skal bare tage sig god tid.
C	Men ellers så har vi din mail hvis der er noget vi kommer i tanke om kunne være rart at få oplyst bedre.
S	Det må I gerne.
C & A	Vil du mene at GDPR lovgivningen er mere specifik og/eller eksplicit ift. persondatahåndtering end tidligere lovgivning på området? (her tænker vi specifikt kravene til virksomheder mht. persondatahåndtering.)
M	Det er ikke nemt at svare entydigt ja eller nej til dette. På den ene side er der selvfølgelig

	kommet nogle nyskabelser til, bl.a. kravet om fortegnelse, konsekvensanalyser, dataportabilitet, ansvar for databehandlere mm., men i bund og grund er principperne for behandling af persondata og kravet til transparens overfor den registrerede de samme. Det er blot konsekvenserne ved at overtræde reglerne, der er væsentligt forøget.

Appendix 5 - Nordea Interview

Participants:

Ellen Pløger (E)
Andreas Hald (A)
Carsten Svaneborg (C)

E	Jamen måske skal jeg lige starte med at fortælle hvem jeg er så.
A & C	Ja meget gerne
E	Altså jeg har været i.., (A opsætter optagelse på mobiltelefon, og E bemærker Nordea dankort) og jeg kan se at du har Nordea betalingskort, det varmer jo ens hjerte.
Alle	Griner
A	Jamen jeg er jo tro kunde
E	Jeg har været i Nordea i rigtigt mange år, mere end 30 år faktisk. jeg er cand merc polit af uddannelse, og har været i danmark statistik, har så været i det der dengang hed atomforsøg anlægget risø, nu hedder det vist energi forskningsinstitutionen risø. og lavet energi og økonomi modeller, og det var egentligt det der bragte mig til banken i sin tid og har siddet i mange år med makroøkonomisk forecast, i en cheføkonom rolle. Men ville så gerne på et tidspunkt bevæge mig tættere på forretningen, (...) og så har jeg efter vi fik den nordiske fusion i 2000, haft rigtigt mange nordisk opgaver, jeg har primært arbejdet nordisk siden. og rigtigt meget omkring distribution, altså hvordan skruer vi et filialnet sammen i en moderne verden hvordan spiller det sammen med nogle online tjenester, hvordan spiller det sammen med et kontaktcenter osv. Og så har jeg de sidste par år beskæftiget mig meget med det emne der hedder hvidvaskning og terror finansiering, som jo har været lidt af et regulatorisk og compliance mæssigt mareridt, for mange banker, også for os. Og så var der nogen der fik den glimrende ide om så ikke GDPR kunne være det næste man kunne kaste sin kærlighed over, og derfor sidder jeg så som den her Group Data Protection Officer (GDPO) hvor den måde vi har sat

	det op på er at vi har en data protection officer (DPO) som er en meget lille organisation, og så har vi et program der kører ved siden af. og jeg tror… de andre i har interviewet har det primært været andre finansielle institutioner?
C	Ja, det har det været, primært større finansielle institutioner.
E	Ja okay, og jeg tror ikke det er noget ualmindeligt setup.
C	Nej, de fleste eller flere har sat et program op til at styre hele GDPR problematikken
E	Ja og det er også det vi har gjort, og så har jeg jo en mere fremadrettet rolle i det her.
C	Spændende
A	Jamen, vores undersøgelser handler egentligt både om den byrde GDPR har været for de større finansielle institutttter, men også hvordan lovgivningen har påvirket dem i forhold til outsourcing, og opbygning af de kompetencer det kræver at være compliant med den her ret radikale lovgivning, øhm ja (A kigger i interview guide) du dækkede meget godt over din historik med Nordea
E	Nej men bare spørg videre, jeg kan sige noget mere om det hvis det er nødvendigt.
C	Jamen jeg tror egentligt bare at vi starter, Sådan helt generelt hvordan har jeres organisation så reageret på GDPR problematikken eller situationen?
E	Ja, som sagt har vi sat det her program op, som er et contralt gruppe program.
C	Hvornår? kan du huske hvornår i har sat det op?
E	Ja vi har haft den første fase som startede for 2 år siden, og så har vi haft en mere intensiv fase som startede i september sidste år. Men som sagt vi er jo en virksomhed, og nu ved jeg jo ikke helt hvem det er i har interviewet, men vi er jo en virksomhed der strækker sig på tværs af ihvertfald norden, og det vil sige vi arbejde meget ud fra at aligne processor, så meget som muligt. der er jo selvfølgelig altid lidt forskel på lovgivning i mellem de forskellige lande, men jo mere vi kan aligne jo bedre. Så det vil sige når vi taler implementering så taler vi meget implementering i hvert af vores forretningsområder, hvor vi har personal banking, vi har corporate business banking osv. Altså den type af forretningsområder som jo i virkeligheden er den type af hovedkunder og det centrale program har så et ben nede i hvert forretningsområde, så man kan sige at

	løsningerne og det der skal løses på gruppeniveau løses af det centrale program, og de føder så løsningerne ned i hvert forretningsområde som så løber videre med det. Så det har været setupet, og som i jo så selv siger så har der jo været utroligt mange komponenter i det her, og nå i så spørger hvordan organisationen har reageret på det, så tror jeg at alle er meget alert på at nu kommer der noget der hedder GDPR, og vi har jo gjort det, som jeg også kan forestille mig at de øvrige i har snakket med også har, at vi har kørt noget mandatory training. for samtlige medarbejdere, netop for at raise awareness. Jeg syntes det man skal huske, det er at okay, GDPR har nogle nye elementer men, der er jo også rigtigt meget der allerede har eksisteret i banksektoren i årevis.
A	Ja det er jo egentligt konsekvensen, eller bøden som er det helt nye.
E	Ja det er på nogle helt andre niveau, og det er nyt, Det er også nyt at vi sandsynligvis kommer til at spille meget mere sammen med data protection authorities, hvor vi jo har været vant til at spille meget sammen med finanstilsynet.
C	Ja data tilsynet skal være kontakt instancen for det her.
E	Ja det står ihvertfald beskrevet i, DPO rollen at jeg skal være kontakt punkt for myndighederne, som i dette tilfælde er data tilsynet, som vi jo ikke har haft særligt meget kontakt med, fordi at al opfølgning på den finansielle sektor har kørt igennem finanstilsynet.
C	Du sagde at GDPR har medført stor awareness omkring persondata, vil du sige om det har været katalysator for generel oprydning af hvordan persondata bliver håndteret eller har det medført andre nye processor.
E	Jeg tror at når der kommer nye reguleringer af den ene eller den anden art, så medfører det jo altid at man går nogle ting igennem, og der finder man jo altid nogle ting, altså helt i den banale ende, jeg har jo gået min mailboks igennem fordi jeg har haft nogle medarbejdersamtaler, og lønninger på medarbejder liggende. for det har ligesom været meget rart at have liggende i et arkiv, og så har jeg ligesom haft “ups jeg tror lige vi rydder op her” så det er klart at den awareness, fører gudskelov til nogle actions, og det er jo klart at det er det samme der sker på systemsiden. For det er jo en væsentlig del af GDPR, at vi skal kunne dokumentere for myndighederne at vi har styr på det, for vi kan godt gå rundt og tro på at vi har styr på det, men det at vi skal dokumentere det er et andet krav. og det er jo klogt nok at bede om for det leder måske op til at man tænker “arh det der skal vi lige have samlet op på”

C	Ja, noteret lidt mer processen for hvordan man gør.
A	Ville du sige, hvis du nu skulle kategorisere GDPR som den udfordring den har været, har det så været en meget meget stor ting for Nordea, eller har det været en mindre ting fordi mange af kravene har ligesom været der i forvejen.
E	Jeg syntes det er fair at sige det har været en stor ting, og det er ikke det samme som at sige at der ikke har været en masse krav i forvejen, men det er klart at GDPR sætter et øget forkus på hvordan vi håndterer personlige data, og specielt afspejler den mere og mere digitale verden som vi er i nu. Og det at få de to ting til og mødes i en mere automatiseret løsning det er en betydelig opgave. Så tror jeg derudover, der er ingen. Ej nu skal jeg ikke tale på andre bankers vejne, jeg tror at der kom, også i kraft af alt det vi har været igennem også på hvidvask og terror finansiering, så er det fokus der generelt er på compliance processor, altså vi har jo flere tusinde mennesker siddende med comliance og terror finansiering. Så det har også medført at “hov nu må vi også lige få styr på det her fra dag et”.
A	Der er også meget fokus på det lige nu, altså over i USA med facebook og privacy er generelt en meget aware ting lige nu.
E	Ja og der er ingen tvivl om, os når man lytter media osv. Men de bruger jo.. det er jo noget oppe i tiden, også fordi GDPR kommer derfor er der jo mere attention på det, men vi har jo ikke set. nej nu skal jeg lade være med at afspore jer, i kører jeres spørgsmål.
A	I forhold til jeres implementering af løsningen, specifikt i forhold til nogle af de her rettigheder, right to be forgotten ret til data indsigt, er det noget i har implementeret automatisk, eller er det noget i gør manuelt?
E	Altså hvis vi nu lige tager right to be forgotten, så skal man jo lige tage den med et gran salt, fordi..
A	Ja på grund af andre lovgivninger?
E	Ja der er så mange andre lovgivninger der forhindrer os i at slette, selvom du så kom i morgen og sagde at du ville slettes. der er skatte lovgivnigen, der er hvidvasknings lovgivningen, der er bogføringslovgivningen så der er en masse ting der gør at vi ikke bare kan slette. og man kan sige at tidsfristerne omkring de lovgivninger har jo ikke ændret sig, og der kører vi nogle automatisk oprydnings rutiner, “den type data her det er 5 år så skal der ryddes på, og den type data her, det er 10 år.” så det er en blanding. Hvis vi tager nogle

	af de andre f.eks right to access, så er noget af det manuelt og noget af det er robotløsninger. Og jeg vil sige nogle af de der rights, det var egentligt det jeg ville sige før. Vi ved jo ikke hvor mange der vil interesserer sig for det. Altså din ret til din data det har du jo i dag, det behøver du ikke vente til den 25 maj for. men der er ingen tvivl om at det kommer mere op, lige nu har vi ikke ret mange hvert år der stiller det spørgsmål.
C	Det kan måske også være fordi der er ret mange der ikke er klar over at det er en mulighed?
E	Tjah, det står i vores generelle vilkår, så jeg tror mere om det kommer op i medierne. Og så kan vi jo risikerer at det pludseligt siger “PUF”
A	Ja og så står de der.
C	Nu var du lige inde på det, men hvor meget af jeres process når i skal udleverer data på en person, men hvor meget af den her process vil være automatisk, og hvor meget vil være manuelt som personer skal ned og grave efter, for at få data frem.
E	Altså størstedelen vil være en automatiseret løsning, men der vil være mennesker henne over det.
C	Kan du sige nogenlunde hvilken procent fordeling?
E	Nej, jeg ved hvor lang tid vi regner med det tager, at der som menneske skal bruges hver gang, men det vil jeg helst ikke sige.
A	Det er også helt i orden.
E	Men altså, hvis ikke det lige pludselig går facebook amok, så føler jeg mig meget komfortabel med de ressourcer vi har sat af til det. og det er jo selvfølgelig også noget med at sikre at det er en standardiseret løsning der kommer så, lige meget hvor man kommer ind i organisationen så er det det samme svar man får ud. Så det er vores operations som laver mange ting der er en blanding af noget manuelt, som også nogen gange er en kvalitetskontrol, og så noget robot automatiseret løsninger, så det er det setup vi har lavet.
A	Hvis vi så kigger på nogle af de kompetencer det har krævet, både nogle IT ting og nogle juridiske ting kunne jeg forestille mig, er det nogle i har haft internt i jeres organisation? eller har i brugt konsulenter? eller har i været ude og hente eksterne systemer?
E	Altså vi har jo haft en del internt, vi har helt klart styrket folk med en del data management

	kompetencer, men det er jo så ikke alene GDPR, det er også fordi data management bliver vigtigere fremadrettet, vi har helt klart gået ind og styrket nogle der har altså kompetencen på data protection generelt, så det er ligesom det interne, og så har vi også haft konsulenter inde, til simpelthen at være arme og ben på noget af det her. og selvfølgelig også bringe nogle kompetencer ind. men simpelthen for at i denne her implementeringsfase og få noget mere kraft ind, så det har vi.
A	Nogle af de IT systemer, er det noget i har bygget selv? eller er det noget i har købt?
E	Altså jeg mener ikke vi har lavet store nye IT implementeringer af hensyn til det her, det har vi ikke.
C	Så i fortsætter med at benytte i store grader den samme data styring?
E	Ja grundstrukturen i det. Og så, og det kan jeg også godt sige for det har været fremme i pressen, vi er igang med at implementere en ny core banking platform, som er under udrulning i finland, og så bliver den derefter rullet ud til de andre lande, så det er ligesom en moderne bank platform, så den har en række af de elementer, så det er den der bliver kernen i det her.
C	Så med hensyn til processerne der bliver lavet, vi har været lidt inde på det, bliver det primært en opdatering af de forhenværende processor eller er der blevet udviklet nye forretningsgange?
E	Øhm, begge dele i virkeligheden, vi har prøvet, eller vi har taget den tilgang at vi til bruge eksisterende processer hvor vi overhovedet kan, og så rette dem til. Altså hvis man tager den hedder privacy impact assessment, som jo er en ny komponent kan man sige, der har vi jo risk processor hver gang vi laver forandringer, jamen så får vi lagt privacy impact assessment ind som et element i den, men grund processen er den samme. Og det er netop for ikke at skulle opfinde noget, der er jo ingen grund til at skulle forvirre gode kollegaer mere end højst nødvendigt. så jo mere vi kan bruge eksisterende processer jo bedre, så det har været grundtanken. men der er jo steder hvor der er nye processer, fordi vi simpelthen ikke har haft de processer tidligere. også for at sikre opdatering af nogle af de elementer som f.eks dokumentation som vi f.eks skal have i orden. Og man kan sige individual rights processerne er jo også, givet at vi forventer at de måske volumenmæssigt bliver meget mere markante. jamen så kan du sige er det nye processor? jamen det er det i et eller andet omfang, og de processer går jo også et er individual rights i forhold til eksternt men de går

	også i forhold til medarbejdere, så det er lidt en blanding, men grundtanken har været lad os lade være med at opfinde noget nyt medmindre det er bydende nødvendigt, så lad os hellere taget noget eksisterende og rette det, og jeg tror meget på at det giver en meget større implementeringskraft, for en ting er at opdatere en forretningsgang, men noget andet er om folk efterlever den. så det er meget nemmere hvis det er en tilretning af noget kollegerne allerede kender.
C	Vil du sige at alle jeres processer når at blive compliant, altså klar, til d. 25 maj? Så hele jeres struktur eller organisation er klar til GDPR?
E	Jeg har ikke mødt nogen endnu, hverken i den finansielle industri eller andre områder, der tør stille sig op på en ølskammel og sige "Yes det er vi". Og det gælder jo alt implementering af regulering at man skal denne her risk-based approach. Hvad er det for nogle ting der er de største ricisi, og så lad os få lagt dem på plads. Altså det der har været væsentligt for os, det er at vi har lavet en plan frem mod 25 maj, og der er de her ting vi skal have på plads og det skal vi nå, og så er der de her ting vi senere skal have på plads
C	Der er 'Need to have' og 'Nice to have', noget i den stil?
E	Ja simpelthen sige at de her ting skal vi have på plads. Og når vi siger de her ting, og ikke nogle andre, så er det baseret på en risikovurdering. Og det gør jo så også at når vi nu ved at vi når 25 maj og har rullet det her på plads, så ved vi at vi står med noget residual risk, som vi skal håndtere efter 25. maj. Men vi ved jo hvad det er. Og det jo vi så, inden 25 maj, skal sikre os at vi har en plan for. At vi ved hvordan vi vil nå det.
C	Og så også evt. kunne vise det til myndighederne som begrundelse.
E	Ja netop, det er en vigtig del af det. Det er jo ikke bare at sige at vi er nået hertil. Det er også at sige at ja vi nåede hertil, men vi ved også at vi mangler de her elementer, men dem har vi en plan for. Men det er ikke bare fordi at 'dem nåede vi bare ikke'. Det er en egentligt beslutning og sige 'det her' tror vi er mere vigtigt end 'det her'. Og så kan man sige, man bliver jo aldrig 100% compliant. Det gør man ikke.
A	Synes du der mangler åbenhed fra datatilsynets side om hvornår man er compliant?
C	Og hvad det vil kræve at være compliant?

E	Altså jeg synes… Altså hvis man læser reguleringen, så er det jo som alt andet regulering. At der er mange hjørner når man dykker ned i det, der kan fortolkes. Og selvom der er det her, såkaldte work party 29, som I sikkert også har stødt ind i, som siger lidt mere. Så udover det, er der jo ikke kommet specielt meget guidance.Og det tror jeg da, med alt respekt, og det er i hvert fald også min erfaring fra hvidvask og terrorfinansiering området, at myndighederne er også på en rejse i det her. Så de skal også finde ud af, hvordan kommer det her til at spille. Så på den måde kan man sige at der er nogle områder hvor jeg godt kunne ønske mig at få lidt mere guidance. Men det er ikke noget jeg har forventninger om på nuværende tidspunkt.
C	Men altså du vil så sige at den vejledning og rådgivning der har været fra offentlig side har været tilstrækkelig?
E	Jeg ved ikke. Altså der har jo været de her forskellige papirer. Men der har jo ikke været meget pro-aktiv rådgivning. Og vi kan jo også se fra alle lande at datatilsynet har jo fået lov til at opruste, altså resourcemæssigt. Så de er jo også lagt under vand på en eller anden måde.
C	Det er jo også en større opgave at begynde at kontrollere sådanne ting, altså GDPR
E	Det er jo så også med til at jeg tror ikke at datatilsynet vil komme d. 26 maj, kigge ned i hjørnene og så knalde 4% bøder.
C	Nej, det er jo også hvad formanden, er det Juncker (Red. Jean-Claude Juncker) han hedder? Han har også været ude og sige at de kommer ikke til at give bøder fra day 1. Det kommer til at være advarsler, en større process der er gradual, osv.
A	De er jo interesseret i at de udøver terror mod virksomhederne, hvor de bare står og slår virksomhederne
E	Nej og jeg syntes også at.. Vi fik jo et par bøder i Sverige på hvidvaskningen. Og det var jo også noget med at de var inden og kigge og så var de inden og kigge igen. Altså de var inde og kigge og sagde 'Ahhh' Og så var de inden og kigge igen og så sagde 'Ahhhhhhhh' ikke? Og det er jo den måde det køre på. Så de jo. Man sender et signal med bødestørrelsen. Og jeg syntes sådan set at det der er interessant ved GDPR og bødestørrelserne, det er jo at der i virkeligheden er lavet en oversigt over [hvad der er vigtigst]. Altså det der koster 4%, det der koster 2% og det der koster 4%. Det er faktisk ret

	unikt ved GDPR.
C	At man kan se præcis hvad det er der koster hvor meget. Så der faktisk er prioriteringer i lovgivningen om hvad der er vigtigst.
E	Ja. Altså fx 'Individual Rights', den er dyr. Ikke? Så på den måde er der i virkeligheden givet noget guidance. Fordi man så dermed sender et signal om det er det her vi lægger vægt på. Og der er et af komponenterne også, at hvis du ikke efterlever indstillinger fra tilsynet. Så er vi tilbage ved, at 'Vi har været inde og set hos dig' og 'Vi har sagt hvad I skal gøre' og nu gør i det stadigvæk ikke. Og nu gør i det stadigvæk ikke. Arh, nu stopper det.
C	Lige præcis. Man løfter pegefingeren et par gange, og derefter må der ligesom komme nogle konsekvenser.
E	Ja.
A	Et spørgsmål jeg godt kunne tænke mig at stille, og du må undskylde hvis det er en smule svært at svare på og det er også helt i orden hvis du ikke kan svare på det. Med hensyn til outsourcing af de her, mht. datastyring. Er det noget i har overvejet at gøre (outsource)? Ved du om det har været til diskussion ifb. med GDPR om man skulle prøve at ligge det ud til en ekstern virksomhed?
E	Det lagde jeg godt mærke til i det I skrev, og det syntes jeg godt nok var et mærkeligt spørgsmål. Så det må jeg forstå jeres baggrund for. Hvorfor tænker I det?
C	Vores initielle ide til det her det var, jeg arbejder i en startup der hedder NewBanking der laver noget med persondatahåndtering. Og det snakkede vi så med vores vejleder om, at det kunne være et interessant emne at skrive speciale om. Og han sagde at det syntes han, men at vi skulle have et mere fokus på generel outsourcing vha. finansielle og regulative lovgivning. Altså hvordan at lovgivningen generelt kan indføre til at virksomheder generelt outsourcer processer. Det er med den tanker, at hvordan en lovgivningn kan være med til at skubbe imod outsourcing og pooling af resourcer indenfor en branche.
E	Så det at det kompetencemæssigt er for dyrt i virkeligheden at bygge det op inden i virksomheden.
C	Ja, så i stedet for at hver større virksomhed har et kæmpe 1000-mand team der laver det samme flere gange, så kan man bruge en fælles provider, i en eller anden stil. På samme

	måde som mange, som e-nettet, på en eller anden måde samler kompetencer. Hvordan lovgivninen så kan medføre eller subbe til at virksomheder benytter sådan nogle her.
E	Altså fordi min umiddelbare reaktion når jeg læste det der spørgsmål, det er at jeg tænkte sådan 'arh altså. Hvorfor skulle de det?' fordi jeg syntes i virkeligheden af noget at det der er kompliceret mht. håndtering af persondata det er jo lige præcis når de ligger udenfor huset. Fordi man skal jo huske at vi stadigvæk er kontroller af de her data. Så vi har ansvaret. Og det er jo der GDPR understreger den her accountability som kontrolleren har. Altså, hvis vi har outsourcet til, fx en del af vores personale håndtering og lønhåndtering, som sikkert mange andre også har, køre uden for huset. Hvis de får knoldet rundt i det, og delt de der data til højre og venstre, så kan vi jo ikke bare læne os tilbage og sige: 'nåh det var dem'. Fordi vi har en forpligtigelse til at sikre os, i en kontrakt, at der er styr på det her. Og vi har i virkeligheden også en eller anden forpligtelse til at sikre os at de overholder det. Så, jeg syntes det er et tve-ægget sværd. Det er klart at der kan komme nogle ting, hvor man siger at det er nogle specifikke kompetencer der giver mulighed for at samle det. Men jeg ser så også i hvert fald mere at, vi bruger jo IBM, det er der så og så mange banker der også gør, ikke. Det er det klart, at hvis IBM får delt, jeg ved ikke hvor mange personlige data, går det så hårdest udover Nordea eller IBM? Nok lidt begge dele, det går i hvert fald også udover dem. Men stadigvæk, det fritager os ikke ansvar.
C	Logikken var også lidt, at når nu der kommer lovgivningen som, i og for sig, klarlægger hvad der er forventet ift. persondataopbevaring, så kan det være med til at gøre det mere generelt, og dermed behøver hver virksomhed ikke at have deres egne specialister indenfor det, hvis det var en mere generelt struktur af håndtering af data, en fælles måde at håndtere det på.
E.	Men der kan det nok også komme lidt an på virksomhedsstørrelsen. Altså hvis vi tager Danmark, så kan vi se at de lokale pengeinstitutter, af gode grunde, går sammen. Ikke? Hvor i en række sammenhænge at Nordea og Danske er så store så nogle ting gør vi selv, fordi vi nemlig har kritisk masse til at have de kompetencer.
C	Ja I har størrelsen til selv at kunne lave det her.
E	Men jeg ved ikke, altså…. Så tror jeg mere vi kommer over i en generelt outsourcing diskussion. Altså hvor meget vil man selv håndtere og hvor meget vil man ligge ud. Jeg ved ikke hvor meget GDPR, for os i hvert fald, bryder den sammenhæng.

C	Der har ikke været nogle diskussion om outsourcing i den forbindelse?
E	Nej det har der ikke. Nu skal jeg ikke fritte jer for hvad andre har sagt. Men har I stødt på der andre steder? Har I set/hørt argumentet for det?
A	Jeg tror ikke jeg behøver at ligge skjul på, at ikke har været vores opfattelse at folk har gjort det. Men vi har også kun snakket med større virksomheder og instutitioner. Jeg tror godt at størrelsen kunne have en indflydelse.
E	Ja det tror jeg også. Det er også min forventning. Det er klart at hvis man er en mindre virksomhed af den ene eller anden art, så kan der være nogle ting hvor man siger, at det kan vi ikke håndtere. Ud med det (red. outsource). Og i den sammenhæng er det jo også understreget i GDPR at den her DPO rolle, det kan man godt sætte en ekstern til at tage. Det kan jo være et revisionshus eller en konsulentrolle. Og det er jo også lige præcist et udtryk for at mindre virksomheder, altså hvem skulle det sætte til det.
C	GDPR er jo også henvendt meget mod større multinationale selskaber. Det er i hvert fald min opfattelse af den
E	Ja men det er jo stadigvæk, mindre virksomheder er jo under sammen lovgivning, så de kan ikke løbe fra den.
a	Mht overvejelser, er det noget i har søgt mening hos andre banker eller Finansdanmark?
E	Der er grupper, eller en gruppe, i Finansdanmark der diskutere de her ting. Og det er jo en lang tradition i den danske finansielle sektor at vi har Finansdanmark
C	Ja som en brancherådgiver.
E	Ja så det har jo meget også i dialog med myndighederne om hvordan skal den kongret spille sammen med eksisterende lovgivning. Og det ene og det andet. Men det er klart at vi kan ikke komme for tæt ind på de konkrete løsningen, for så kommer vi i kambolage med konkurrencelovgivningen. Altså der er en hårfin balance i de her ting. Fordi vi må ikke sidde et eller andet sted og sige, nå ja.
C	Ja 'så gør vi alle sammen sådan her'
E	Ja det er der hvor man lige skal tænke sig rigtig godt om. Men det er klart at der ligger nogle rent praksiske ting som man ligger diskutionerne opad i Finansdanmark.

C	I forlængelse, har I set hvad de andre banker gør og så justeret jeres håndtering ift. til det? Altså jeres konkurrenter.
E	Altså jeg kan ikke nævne et konkret eksempel på det. Jeg tror egentligt mere at det er om at snappe lidt information op, og det behøver ikke være i Danmark vel? Vi har jo de andre Nordiske lande hvor vi hører hvordan det foregår og vi høre jo i det international miljø hvad er oplevelsen, hvad har man gjort osv. Så det er det man bliver inspiration
C	Så I har brugt jeres størrelse til at have følere ude i de forskellige lande for at få et generelt konsensus over de forskellige lande?
E	Jeg vil ikke sige generelt konsensus, men mere forskellige indtryk at bygge på. Så det er mere, "Hvordan gør andre, hvordan sætter de det op, osv". Det er man selvfølgelig meget nysgerrig over. Og det er jo konferencer og roundtables, osv. Som også giver mulighed for at få en fornemmelse for hvordan andre tænker osv. Det genrelle billede er jo at alle, på tværs af sektorer og hvilke lande, så er alle 'bambi på isen' her, og bevæge sig fremad, men som jeg også sagde før, der er ingen der tør stille sig op på en ølkasse og sige 'Yes! Vi er done'.
C	I forbindelse med det her, ser I så persondatahåndtering som en 'cost of doing business' eller som en konkurrencefordel
E	Jeg vil sige begge dele. FOr det er klart, at det er lovgivningen og så er det sådan det er. For hvis du går tilbage til hvidvask og terrorfinansiering så har det immerhen også været dyrt. Men sådan er det. Om det er en konkurrencemæssig fordel, det ved jeg ikke. Jeg ser sådan på det at det her er et spørgsmål om tillad. Og når du i hvert fald kan jeg se (henvisning til A som er Nordea kunde), har delt nogle data med os, så skal vi sørge for at vi passer på dem og at vi kun bruger dem til det vi har aftalt. Vi skal sørger for at der ikke er nogen der kommer ind og napper dem. Så det er tillid. Og hvis det sker at vi laver en 'breach of personal data', og det sker jo, en kurvert hvor der kommer de forkerte dokumenter i jo, det behøver ikke at være det store Cyper Attack vel?
A	Nej, fx en telefon der bliver stjålet
E	Præcis! Altså, whatever it could be. Så er tilliden mellem kunden og virksomheden under pres ikke? Og det er jo i høj grad hvordan håndtere man den situation når det sker ikke. Siger vi det til dig, siger vi det ikke til dig.

C	Det er jo også der hvor GDPR har sagt retningslinjer for hvornår man skal underrette myndigheder og individer?
E	Myndigheder skal underettes og i nogle tilfælde skal data subjects underettes. Og det er jo lige præcis at hvordan hpåndtere vi de situationer. Og det der hvor vi gerne vil have åbenhed omkring det. Og altså 'Sorry, det skete'. Men det er det her der skete og det er det her vi har gjort. Det er vigtigt. Og det er derfor tillad, og det er jo en konkurrence parameter.
C	Helt klart. Det er jo en form for brand.
E	Facebook er et meget godt eksempel pt. Og det er jo den gamle sandhed, at det tager utroligt lang tid at opbygge tillid men det tager 2 sekunder at ødelægge den på. Så man skal tænke sig godt om. Og der er det jo klart at når vi skal inberette til data tilsynet hver gang vi har en breach, så tvinger det jo også os til at reflektere og kigge indad.
C	Få registreret hvad der skete, hvor det skete, hvordan osv
E	Yes. "nu er det præcis det samme som skete for 3 måneder siden, det kunne være vi skulle kigge den process igennem igen." Så der er elementer at 'det skal vi bare gøre' og elementer af tillid. Og det gælder jo alle, det nytter ikke noget at være fornærmet ovre i hjørnet, for de andre har samme vilkår.
C + A	Vil du mene at GDPR lovgivningen er mere specifik og/eller eksplicit ift. persondatahåndtering end tidligere lovgivning på området? (her tænker vi specifikt kravene til virksomheder mht. persondatahåndtering.)
E	Jeg mener, at GDPR lovgivningen er mere specifik end tidligere. Jeg tænker først og fremmest på kravene til at kunne dokumentere ("demonstrate"), at processing foregår i overensstemmelse med reguleringen (Article 24.1). Det er samtidig klart, at mange måske ville ønske, at der var nogle klarere beskrivelser af, hvad der skal gøres . Det er imidlertid her, at det er op til den enkelte virksomhed at beslutte, hvad der er nødvendigt i relation til "technical and organisation measures" for at beskytte "rights and freedom of natural persons" med baggrund i den virksomhed, som man driver.

Appendix 6 – Danske Bank Interview

Participants:

Andreas Hald (A)
Carsten Svaneborg (C)
Jens Klæbel (J)

C	Yes, men som sagt tusind tak fordi vi måtte komme
J	Jamen velbekomme
A	Jamen skal vi lige starte med at fortælle lidt om os, Vi er ved at skrive vores speciale, vi læser Cand Merc IT ude på CBS, det er lidt samspillet mellem økonomi og it og derfor var det meget oplagt for os at nu hvor der kommer en lovgivningen der fra et IT perspektiv er meget spændende, så prøve at se hvordan den har indflydelse på større finansielle institutter. Og der falder i jo meget godt i den kategori. Så lidt mere specifikt prøver vi at se hvordan denne lovgivning har påvirket jer i forhold til nogle af de kompetencer den kræver.
J	Yes, men. Jeg hedder Jens Klæbel, jeg har været i banken i 20 år, Jeg har arbejdet med IT i mange år, mange mere end det. Jeg har en baggrund som datalog fra københavns universitet. Og har arbejdet som leder her i altid, og lige nu sidder jeg og styrer det der hedder vores regulatory ting, compliance. Primært AML, Primært GDPR og så også nogle andre ting. GDPR er en stor ting for danske bank, det er der ingen tvivl om, det er et 3 cifret millionbeløb vi investerer i det. For at få det på plads. Og det gør vi af mange forskellige årsager, den primære årsag er at vi ønsker at være compliant med lovgivningen, vi ønsker som udgangspunkt at være i overensstemmelse med al lovgivning. Men vi ser også nogle fordele i at køre løs med GDPR. Vi kan se at betydningen af data er stigende, og derfor så bliver betydningen af at man kan passe på folks data, og behandle dem ordentligt også vigtigere. I kan se bare facebook nu her med Cambridge Analytics.
A	Ja lige præcist det er også meget oppe i folks opmærksomhed lige nu, derfor er det også oplagt.
C	Ja det hele ramler ligesom sammen, facebook har en kæmpe privacy sag, GDPR

	lovgivningen som revolutionerer den europæiske data lovgivningen, og generelt folks øgede opmærksomhed på persondata.
J	Så der skal vi jo selvfølgelig være med, folk kommer jo til os med meget forskellige oplysninger, og nogle er mere følsomme end andre. Der er jo mange forskellige oplysninger som vi kan hive ud på forskellige måder som er helt almindelige dagligdags oplysninger, hvor der jo ikke er nogle der vil sige "arh det er da også ligemeget" og så er der selvfølgelig andre oplysninger der kan være mere følsomme, i det helt følsomme område har vi f.eks sunhedsoplysninger, Danica er jo en del af koncernen. Og i Danica har man jo pensionssager man har en sundhedssikring, en kritisk sygdoms forsikring, hvor man skal afgive oplysninger om din sunhedstilstand. Og sunhedsdata det er jo særligt følsomme data i GDPR forstand. Så er der jo data som f.eks Kredit data, din kredit score din kredit værdighed. Ansøgning om diverse lån og sådan nogle ting, jeg tror ikke de er følsomme i GDPR forstand, men de er jo personhenførbare.
A	Ja det er det der er termet.
J	Men i en bank mæssig forstand er de jo følsomme, det er de færreste der ville se sig selv hængt ud på nettet, "nåh så søgte han om 2 en halv million til huset, og det fik han ikke for det havde han sgu ikke råd til"
S	Ja det er meget private oplysninger
J	Ja lige præcis, så den situtation vil vi selvfølgelig nøde ud i. Så derfor har vi sat et kæmpe program igang, for 2 år siden. og nu kører det bare på fulde drøn
A	Det er også lige ved at være oppe over.
J	Ja
A	Hvis vi kigger lidt mere på de interne kompetencer det har krævet, er det noget i har påtaget jer selv?
J	Ja, Vi har ikke outsourcet noget, vi hyrede en gut ind som har beskæftiget sig meget med GDPR tidligere, til at drive programmet på forretningssiden. En der hedder Ole Steen Brems. Fordi en stor del af opgaven ligger jo også i forretningen. Og han har stået for at lave en egentlig afdækning af hvor har vi vores data hende. for selvom vi sidder her i IT så er det ikke sikkert vi ved det, fordi rundt omkring i organisationen der er forskellige øer af

	data. Det kan jo være der er nogle der trækker forskellige regneark ud og har dem liggende. Det kan være over dem der har søgt et job, eller det kan være over dem hvor man egentligt godt kunne have lyst til at sende en mail, "kunne du ikke have lyst til at købe det her lån" eller sådan noget.
A	Der er det jo det sværeste at tage hånd om, sådan programmatisk.
J	Præcist det er alle de der regneark der ligger rundtomkring, eller det der er værre. Mailservere, eller SSAS dataset. Så det har vi lavet en stor afdækning af, hvor vi har været ude og snakke med samtlige forretningsenheder for at se hvad der ligger. For så at kunne lave en GAP analyse for at se hvor vi står på de forskellige krav i lovgivningen. Og så har vi jo så ud fra det foretaget en risiko afvejning for at sige her vil vi holde fokus, og her okay der vil vi måske gøre det så godt vi kan, men det kan da godt være der er nogle der vil syntes det ikke er godt nok senere hen. Men når vi kigger i de vejledninger der er kommet fra datatilsynet, så er der jo ikke megen hjælp at hente
A	Net har også været det indtryk vi har fået når vi har været ude og interviewe, at der har manglet lidt en klar retningslinje og hvad er acceptabelt.
J	Ja det kan man vist roligt sige, at den mangler. Og så har vi jo truffet nogle valg selv, og så må vi jo sige at det er fint, det kan selvfølgelig godt være at vi kommer i uføre på et tidspunkt, og så er der noget som vi må gøre bedre. Og så må vi jo tage den og håbe at de ikke er i dårligt humør og udsteder en bøde. De kan vel også godt lige læse indad, og se at de ikke selv har været helt skarpe på vejledningerne. Så det ville være unfair at komme ud med bål og brand
C	Ja formanden for organisationen mener jeg har været ude og udtale at de ikke bare kommer ud og begynder at udstede bøder, men der kommer advarsler osv i første omgang.
J	Men i og med at vi har godt fat i alt, så mener jeg også at vi er istand til at hvis der er et område hvor de kommer og siger, det her der er i ikke gode nok. Jamen så mener jeg også at vi har kraften til at flytte os på det område. Men der hvor vi har valgt at satse, Altså vi har jo valgt at vi ikke vil outsource.
C	Må vi spørge lidt ind til det?
J	Ja endelig

C	Har det været til diskussion om der skulle outsources noget?
J	Nej, det har det ikke været. Det eneste vi har gjort er at vi har hevet nogle eksterne konsulenter ind. Jeg tror vi hev en 15 litauiske konsulenter ind.
C	Indenfor hvilket område er det så?
J	Jamen det er indenfor forretningsgange og træning
C	Sådan legal compliance?
J	Yes, og skrive og opdatere forretningsgange, være med til at udarbejde noget træningsmateriale. lave forskellige dataudtræk, så det har alene været noget hvor vi har skullet have nogle arme og ben til at hjælpe os. Ellers har vi ikke gjort noget. Vi har selvfølgelig været i dialog med forskellige foretagender, Vi har været i dialog med Bruun og Hjejle, vi har været i dialog med KPMG. Men altså det har været en løbende dialog hvor der har været noget 'ping pong', nu hvor der ikke har været noget fra data tilsynet så hvor står vi henne?. Vi har været i dialog med IBM om det, og så har vi taget nogle forskellige reference besøg, et med en finsk bank og et med en belgisk bank, og så har vi også været lidt rundt i danmark. for at se hvor står vi.
C	Ja hvad er niveauet. Med hensyn til at i ikke har valgt at outsource, er det fordi i generelt ikke outsourcer?.
J	Ja, det kan man sige, i danske bank, der er der ligesom et pendul der har svinget, meget hvor vi for måske 8-10 år siden outsourcede meget, vi outsourcede f.eks hele vores it drift til IBM, den har vi insourcet igen.
C	Ja det er også indtrykket man har som ekstern
J	For nogle år tilbage, og det stod jeg faktisk selv for, der insourcede vi vores IT i indien, vi havde outsourcet vores IT til en virksomhed der hed ITC, indian tobacco company, de havde et selskab der hed ITC infotech. de leverede it kompetencer til os, og på et tidspunkt havde vi 700 it konsulent siddende i indien. Der besluttede vi os for, vi havde nemlig i klausul i kontrakten som gjorde at vi kunne købe deres folk i et eller andet omfang. og det gjorde vi så og oprettede vores eget it selskab, og nu har vi så vores eget it selskab dernede det hedder Danske IT, i bangalore med 1000 mand.

C	Ok, så de klarer simpelthen al jeres IT drift?
J	Så det er simpelthen insourcet, og de klarer så it udvikling, it vedligehold. og Driftsopgaver klares så herfra.
C	Må jeg så spørge rent teknisk hvis al jeres IT drift er i indien er der nogle proble...
J	Nej den er ikke i indien, vores IT drift er her og i indien, udviklingen er i lituan, her og indien.
A	Med hensyn til GDPR, den her større invistering du fortæller i har lavet, har det været i at opdatere gamle systemer, eller har det været udvikling af nye.
J	Det har været opdatering af gamle systemer, ja vi har ikke udviklet noget nyt.
C	Hvad med forretningsprocessor, opdatering?
J	Ja det har været opdatering af processor og politikker. Og i samme lejlighed der har vi også brugt GDPR som lidt en sneplov til at rydde nogle ting op. fordi en virksomhed med danske banks alder og størrelser, der er der jo noget der ligger og roder rundt omkring. Så vi har brugt GDPR som lidt en sneplov til at få rettet nogle ting op. og en af de ting vi har rettet lidt op og såsom politikker processer og forretningsgange. og dem får vi så over i et system, det har før været spredt lidt rundt, og nu får vi det så samlet et sted.
C	Så det vil sige at GDPR har været en form for drivkraft.
J	Ja det har været en katalysator for, og så har den ligesom også været en fundingsmekanisme, så samtidigt med at vi sikrer at vi er compliant så rydder vi altså også lige op. så slår vi 2 fluer med et smæk og nu er pengene der til det.
A	Ja når der ikke er fokus på det så er det svært at søge op til bestyrelsen og bede om penge.
J	Ja lige præcis, vi skal bruge en masse penge på at rydde op det er der ingen der gider. Og det samme gør vi i data, det er der vi har lagt vores vægt på at sikre at vi ikke opbevarer data vi ikke må opbevare. Der er jo forskellige hjemmel til at opbevare data, og så er der en bogføringslov som også fortæller noget om hvordan data skal opbevares. og den overruler jo persondata forordningen. Men de data hvor der ikke er noget hjemmel for det, eller hvor hjemmel er udløbet, jamen der sørger vi for at få ryddet op. Det er et

	fokusområde, så har vi et til fokusområde, for vi har en teori om, jeg ved ikke om det er rigtigt, men vi har en teori om at vi kan blive mødt med, et krav af folk der lige vil teste os af. ikke den 25, men de går måske ind i banken mandag der d. 27 eller 28 maj og siger nu vil jeg gerne se hvad i har på mig. Og det ved vi erfaringsmæssigt f.eks at i UK er det meget udbredt at man gør det. Og der kan vi bruge rigtigt lang tid på at finde de data frem, så det har vi haft meget stort fokus på at automatisere, Så når man går ind i banken d. 28 maj vil man kunne få en rapport
C	indenfor?
J	Indenfor de 30 dage som der er i loven, men i virkeligheden arbejder vi på at det er instant, og du kan få den i hånden ved tryk på en knap.
C	Og det forventer i at have nogenlunde klar til..
J	Det forventer vi at have nogenlunde klar d. 28 maj.
A	Det er imponerende
J	Samme med data portabilitet, at kunne udlæse på et maskinlæsbart format de data som folk selv har indleveret. Vi kommer ikke til at udlevere usb stik, men så kan man få et regneark tilsendt i sin netbank eller mobilbank
C	Og det kommer til at basically være en 100% automatiseret process
J	100%, så er der jo selvfølgelig nogle ting.
J	Jeg går ud fra at der er en vis fortrolighed her, ikke?
Begge	Yes det er der.
J	[redacted]
C	[redacted]

	[redacted]
J	[redacted]
A	[redacted]
J	[redacted]
A	[redacted]
J	[redacted]
A	Er det en bekymring I har, at man vil gå ned en gang imellem og få et udtræk?
J	Nej ikke en gang imellem, men at der kommer et run umiddelbart efter d. 28 maj. Jeg ved ikke om det er en bekymring,
C	Nah det er vel en faktor man bare skal tage med
A	En af de andre banker vi snakkede med, fortalte at de var meget bekymret for journalister.
J	Ja det har vi også tænkt over. Og vi regner da med at der kommer nogle journalister der vil komme og bede om data. Men der tror jeg at det er de færreste journalister har nogle af de lidt mere avanceret produkter. Så de får hvad de skal have, og så er den på plads. Så er der jo også en anden ting, som vi også arbejder på at få på plads. Og hvor vi også arbejder på en simplificering af samtykke. Hvor vi sikre os at dels, får vi simplificeret og reduceret antallet af samtykker, for lige nu er samtykke en del af vores almindelig betingelser. Men der er lille krølle ved samtykker og det er at det skal være lige så let at hive det tilbage som det er at give det. Og det arbejder vi også på, og det regner vi med at have en løsning på, her d. 28 maj.
A	Hvad med ret til sletning af data. Har det været en stor udfordring? For som bank, der

	ligger i jo i et lidt sjovt mellemspil, for der er jo nogle lovgivninger der siger at data skal I gemme og andre siger i skal slette dem.
J	Det er en udfordring. At man hele tiden skal finde ud af hvornår, og hvordan og hvorledes. Og så skal vi jo også, når vi skal slette data så skal vi egentligt også ud på vores papirarkiv og finde dem. Hvor vi jo også makulere nogle papirer. Vi har jo også et stort papirlager liggende i Ishøj. Så har vi en hel del i Danica liggende på Microfish
A	Hvad er det?
J	Det er mikrofilm.
C+A	Nå okay!
J	Nu er i ikke så gamle, men i gamle dage når man gik på biblioteket, så kunne man ligge en mikrofilm ind i et apperat og så kunne man få et indeks over hele biblioteket. Der har vi lagt noget ned på mikrofilm der. Det kan vi ikke gøre noget ved. Og det tror jeg også vi har hjemmel til, hvor ellers skulle man sidde med en saks og klippe ud af microfilmen. Så der har vi noget der.
C	Er det en legacy ting, eller er det en 'off-the-grid' backup?
J	Det er en legacy ting, der er helt fjernet fra det elektroniske. Det er en ren arkiv ting, i stedet for at have det på arkiv.
A	Der er vi jo også inden for, at indenfor en årrække vil det data I har på personer jo stille og roligt blive forældet. Du snakkede jo lidt om at I havde søgt at aflæse hvad det acceptable niveau for dette var. Du snakkede lidt om England, men også at det var andre banker i Danmark, vil du uddybe lidt jeres position?
J	Ja det har vi primært gjort gennem Finansrådet.
C	Så deres arbejde og deres workshops har været med til at influere jer?
J	Yes. Og vi har selvfølgelig plads der. Og vi har en gut der er jurist og er vores mand derinde. Og han har jo været der og hørt hvordan de andre banker har gjort og bragt det med tilbage. Og ikke i en kartel dannelses forstand selvfølgelig.

C	Nej det er klart. Mere i en sektor vidensdeling
J	Ja lige præcis.
C	Du nævnte at der har manglet informationer direkte fra datatilsynet eller fra den regulative arm. Men Har datatilsynet haft en holdning? Og hvordan har den holdning influeret jeres beslutninger?
J	Jeg har ikke selv været med til det, så det er 2. hånds informationer. Men vi har haft et møde med data tilsynet og det er mit indtryk, at det var et møde der forløb stille og roligt og ikke gav anledning til nogen bekymring. Men jeg tror at det var et jurist møde, så ehh.. Hvad de har nærmere talt om eller aftalt ved jeg ikke. Jeg har bare ikke hørt noget der skulle være alamerende.
C	Og hvis vi tager nogenlunde samme spørgsmål mht. Finanstilsynet. Om de har haft nogen holdning eller om de har været ude og sige...
J	Vi har ikke hørt noget fra Finanstilsynet om det her. Overhovedet. Mig bekendt. Der kan være ting der ikke har været kommet forbi min næse. Vi har ikke hørt noget noget som helst.
A	Der er også lidt modstridende interesser ikke?
J	Ja. Det overlader de formodenligt 100% til datatilsynet.
C	Ja som kommer til at være den udøvende magt.
C	Det var nogenlunde de spørgsmål vi havde. Har du noget du føler kunne være relevant for os at vide mht. GDPR eller andre regulative initiativer der har medfør forandring i jeres organisation?
J	Altså. Generelt ser vi der er meget regulativt. Vi har en portofolio af regulatioriske projekter som er ret stor, den har en værdi på over en halv milliard på IT siden. Vi bruger over en halv milliard på regulatoriske ting og sager. De 3 største, arh de 2 største, er GDPR og AML. Så har vi en efterbrænder på MIFID omkring værdipapir handel og information til kunder omkring værdipapirhandel. Og så har vi jo selvfølgelig noget på PSD2 en vis indsats. Og så er der også et par andre områder.
C	F.eks. sådan noget som AML, der har vi jo AML4 lige nu og det kommer i 5'eren der er

	under udarbejdelse. Og det følger I vel tæt med i?
J	Ja! Meget, meget tæt. Det behøves jeg vist ikke at sige. Meget tæt. Vi er meget, meget opmærksomme på AML.
C	Kunne du, eller kunne Danske Bank, forestille sig outsourcing i nogle aspekter indenfor de kommende lovgivnigns typer? Eller hvis der måske bliver lagt op til det?
J	Nu er vi jo en stor spiller på markedet. Så vi kan det meste selv. Men jeg hørte om nogle på markedet der var i gang med at lave DPO as a service. Data Protection Officer. De var igang med at lave noget at det som en service,. Men vi ville aldrig benytte os af sådan en service, vi ville have vores egen DPO.
C	Og det er simpelthen fordi at I er store nok til at kunne gøre dette her selv.
J	Ja vi er store nok, det er hovedargumentet.
J	Ehm. På AML siden, der bruger vi jo forskellige levenrandører. Vi bruger dem til fx at levere skaningsværktøjer og monitorerings værktøjer, men vi har ikke outsourcet noget af det. Der har vi så gjort det på AML siden at vi bruger ret meget tid på at kigge kundedata igennem. For at lave den her KYC, og der har vi oprettet et center i Lithauen, hvor vi har adgang til meget dygtige folk, men til en tredjedel af prisen. Halv pris til en tredjedel af prisen. Og meget dygtige folk. En lidt anden arbejdsmorale.
C	Er de processer så stadigvæk in-house?
J	Ja de er stadig inhouse. Det er stadigvæk en del af Danske Bank koncernen. Og der har vi så, hvad skal man sige, et relativt stort center med flere 100-mand der kan gøre disse ting for os. Det er en form for inhousing/outsourcing. Ja en slags nearshoring. Men vi har baere stadig selv kontrollen med det.
C	Hvad med systemer? Er det selvudviklet systemer eller hvordan?
J	Det er købesystemer eller selvudviklet systemer, eller en god blanding. På AML der er det selvudviklet systemer på alt omkring KYC og alt omkring transaktion monitorerig. Mens transaktion screening, som er der hvor man inden betalingern går igenenm tjekker om den er ok, det er købesoftware. Custoemr Screening er købe software. Også fordi det hænger meget på den data der kommer fra forskeligge offentlige kilder. Fx EU, fra USA, deres

	treasury, UN, osv. Sanktionslister over skurkene i denne verden.
C	Og diverse PEP lister mm.?
J	Ja og PEP lister mm. Det kommer ligesom med værktøjet. Vi bruger også noget værktøj til ligesom at lave nogle investigations. Der bruger vi sådan lidt der kan håndtere store data mænger.
C	Ja, potentielt også noget A.I indover?
J	Jaerh, det lugter lidt derhenaf.
C	Måske mere noget machine learning?
J	Ja det er liidt af det i det,. Men ellers har vi ikke outsourcet noget. Nah, kan ikke rigtigt komme i tanke om noget. Vi insourcer ting. Vi insourcer ting. Vi insourcer ting. Og så flytter vi opgaver hen hvor vi har kompetencerne til det. Fx til Lithuan. Samlet 2.000 mand i Lithuan. Det er jo en meget stor work-force samlet i Lithuan, som jo ikke er så stort et land. Og det er både IT folk, og forretningsfolk. Og vi har jo 1.000 mand i Indien.
C	Hvad med sådan noget som PSD2, som jo åbner banken op. Vil der være nogle kondsekvenser ved jeres insourcing strageti? Meget vil måske kunne laves af andre 3. parter?
J	Ja det vil vi gerne. Vi vil gerne have at 3. part kommer ind og leger med os. Og laver aggregeringsløsninger mm. til os. Det er det vi ligger op til. Og jeg mener også at vi har et betalingsinterface, API, ude nu, for udviklere. Jeg er ikke 100%, men det mener jeg. Som man kan lege med i et sandkasse niveau. Vi har jo skilt os af med Mobile Pay, som nu er et seperat selvskab hvor de andre banker har købt sig ind. Mobilepay har jo den aggregator rolle. Og det er vi jo glade for, for vi er stadig storaktionær i foretagende. Men også andre der kan komme op med noget godt, for kigger man ud i den store verden er der jo masser af gode ideer.
C + A	Vil du mene at GDPR lovgivningen er mere specifik og/eller eksplicit ift. persondatahåndtering end tidligere lovgivning på området? (her tænker vi specifikt kravene til virksomheder mht. persondatahåndtering.)

J	Det kort svar er: ja. Et lidt længere svar er nok nærmere: Den gældende persondatalovgivning indeholder allerede en stor del af det, som er GDPR kommer med, så forskellen er i sidste ende nok så stor. Den store forskel er bøderammerne og den øgede bevågenhed i medierne som følge af forskellige datalæk og diverse udfordringer med sociale medier.

Participants:

Andreas Hald (A)
Carsten Svaneborg (C)
Hanne Roliggaard Andersen (H)
Simon Frank Wendelboe (S)

Person:	Quote
A	Ja, men vi kunne jo lige kort starte med at fortælle om os, vi er jo igang med vores speciale nu, og vi kunne godt tænke os at vide noget mere om GDPR, specifikt hvordan den har påvirket større banker.
C	Så falder hele deadlinen jo med GDPR, som passer perfekt med vores speciale, og det er spændende da den jo har kæmpe impact på mange industrier, og ja specielt banker som jo har meget persondata
A	Ja og hypotesen er der at vi tror at det i højere grad har påvirket banker til at outsource kompetencer i modsætning til at insource.
C	Ja vi vil ihvertfald gerne se om det er noget der har sket. øhm, persondata er meget følsomt, så hele opbevaringen af det er meget følsomt, og så er der jo mange andre regulativer, specielt i en bank. omkring hvad man kan og ikke kan med persondata
H	Så hypotesen er at man ville outsource lagringen af data?
S	(S ankommer i lokalet)
S	Hej, Simon
C	Hej, Carsten
A	Hej, Andreas
H	Det var godt
S	Beklager lige forsinkelsen

A & C	Det er helt fint
H	Ja jeg vidste du ville have meldt afbud hvis ikke du kunne
S	Ja, nej. Det er jo lige så mange andre ting man skal holde styr på
H	Ja vi startede jo bare lige helt kort
C	Ja, vi kan jo lige starte med at fortælle igen hvem vi er kort. Jeg hedder Carsten og det er Andreas, og vi kommer ude fra CBS. Vi læser en Cand. Merc IT og er i gang med at afslutte vores kandidat med et speciale. Og det skriver vi om GDPR problemmatikken og hvilken betydning den har for banker og den finansielle sektor. Og hvordan banker håndterer denne lovgivning og om outsourcing har været et element i det. Også generelt om lovgivningen har været en indflydelse i om man skal outsource eller insource
S	Det lyder spændende, Nu siger i problematikken, eller i bruger den wording - Ja man kan jo forstå en problematik på mange måder, er det et specielt paradigme i forhold til det?
A	Nej øh, vores udgangspunkt er at blive compliant med lovgivningen, og det er jo selvfølgelig også et vagt ord, for det er også en gradbøjning. Jeg tror nogle af de andre stedet vi har haft fat i der har det her med outsourcing været relevant, eller ihvertfald brug af konsulenter har været en stor del af det. og formuleringen af lovgivnignen har vi på fornemmelsen har været en del af det.
A	Men jeg ved ikke, vil i ikke kort lige starte med at fortælle lidt om jer selv, og jeres stilling herude (Nykredit)
S	Øh jamen jeg hedder jo simon, og jeg er ansat oppe i GDPR programmet, vi har opsat et helt program herude omkring persondata. Jeg er ansat i programmet som ansvarlig for hele vores rapporteringsdel så vi får tracket de ting der skal måles på i forhold til fremdrift, i forhold til at kunne rapportere både interne og eksterne interessenter, styregrupper osv. Jeg har haft en lang historie med mange forskellige jobs internt i koncernen, hvor jeg har et stort og bredt kendskab til mange forskellige ting i organisation. og det har jo selvfølgelig givet mig en god ballast og indsigt i mange af de problematikker og udfordringer som vi har stået overfor. Så det var sådan lige meget kort.
A & C	Ja

H	Og jeg sidder i vores digitale marketings afdeling, og har gjort det i mange år, i sådan lidt forskellige konstellationer, men altid med fokus på markedsføring. Og crm delen. Så kan man jo sige hvad laver jeg i et GDPR projekt? men det er jo fordi at helt overordnet i koncernen har man udvalgt nogle spyd spidser, sådan at man får dækker alle hjørner af koncernen, og der er jeg så spyd spids for vores hjørne af koncernen. Også alene navnet på vores afdeling siger at vi har rigtigt meget data, vores apps, systemer alene kundedata, der er bare rigtigt meget data man skal forholde sig til. Så jeg sidde og prøve at holde styr på de 40 mennesker der sidder deroppe og bruger data.
S	Sådan for lige at give et kort recap af hele programmet. Så er det jo endt i den konstellation af et overordnet program som har 6 sub projekter nedenunder, og hver enkelt sub projekt har hvert sit eget område. Men vi skal ud og røre ved hele organisationen, modsat til mange andre compliance eller regulative projekter som vi har været underlagt. Og i denne omgang har det været godt at have en som Hanne, som er god at have ude i de forskellige enheder, og selvom som jeg sagde før at jeg har et godt kendskab til hvad der sker ude i organisationen, så er jeg ikke nede i deltajerne, jeg har en fornemmelse af det. Men det er jer der ved det (Taler til Hanne).
H	Jo for man kan jo sige det handler ikke kun om at man skal være compliant d. 25 maj, vi skal også have indarbejdet nogle arbejdsrutiner fremadrettet så vi ikke står i den samme lort til halsen om et år. Så det handler det jo også om.
A	Ja lige meget hurtigt, hvor mange år har i været her i nykredit?
H	Jeg har været her siden 2001
S	D. 25 maj, dagen før GDPR har jeg været her i 10 år
Alle	Griner
H	Det er jo simpelthen et tegn.
Alle	Griner
S	Ja jeg troede det var løgn da jeg så det.
A	Jamen i forhold til GDPR, hvis i bare skal sætte nogle generelle ord på, hvordan har

	Nykredit så reageret på denne her lovgivning?
S	Jeg vil sige at nu, at det er jo en form for regulation den her, og den finansielle sektor har måske en fordele i forhold til andre virksomheder i danmark, da vi er forholdsvis hårdt reguleret i forvejen. så derfor rammer det nok ikke os lige så hårdt som det gør for andre.
C	Fordi i allerede har været vandt til det?
S	Ja vi har allerede en compliance afdeling, og vi er vandt til at det er en del af vores dagligdag, for at vi kan få lov til at åbne op om morgen, jamen så skal vi leve op til nogle ret stramme krav. så nu skal vi bare leve op til et nyt krav. Men samtidigt må vi også erkende, at det er ikke sådan at nye krav altid bare bliver taget imod med åbne arme, selvfølgelig kan det skabe noget ramaskrig, også fordi det nok er den første regulering der rammer hele organisationen. Alle andre som mifid, eller hvidvask osv, jamen det er nogle der ligger i nogle specielle områder eller en bestemt gruppe er medarbejder. Med denne er vi ude i hele organisationen og til alle medarbejdere.
H	Og det syntes jeg måske har været en del af udfordringen, ikke. for ude på centrene som arbejder med kunderne, de er jo vandt til det. og jeg tror for dem der er det bare et addon til alt det andet. Men for mig, jeg repræsenterer jo nogle der ikke er vandt til det, og for mig. Det skal vi jo virkeligt have fat i nakke skindet på dem. Det er ikke nemt.
S	Som mennesker er vi jo interesseret i vores arbejde, og den måde vi selv syntes vi gør det bedst på. Så når der er nogen der kommer og siger jamen du må ikke behandle data på den måde du har gjort før, jamen så kan vi godt føle os en smule personligt krænket, og det forstår vi godt hvorfor der er mange ude i organisationen der gør. At man skal beskæftige sig med ting som man ikke er vandt til som at rydde op efter sig selv. Det er ikke altid lige så sjovt.
A	Nej og den sætter jo også en masse krav overfor hvad jeres kunder kan kræve af jer, det her med at slette data og udlevere data.
S	Det er rigtigt
A	Har det været, er det noget i har gjort tidligere?
S	Det er noget den nuværende lovgivning også tillader, man kan under den nuværende

	lovgivning godt søge om tilladelse.
H	Det tror jeg ikke rigtigt, har det været brugt?
S	Nej kun i meget lille målestok, så har det været sure kunder der siger slet alt om mig, eller giv mig alt hvad i har. Nu formaliseres det jo bare under forordningen, hvor der er nogle regler der siger at man skal have respons indenfor en periode, og hvis ikke man har fået det, eller hvis kunder ikke får respons, så kan man udsætte det, men kun under nogle skærpede omstændigheder.
C	Hvad med sådan nogle, der er jo også andre lovgivninger inde over disse områder, hvad med AML den siger jo også at man skal gemme ting nogle år efter. Der tager dette jo overhånd over GDPR.
H	Ja det overruler altid.
C	Så det skal man jo også tage højde for.
H	Ja men det tager man jo også højde for, vi er igennem jeg ved ikke hvor meget e-learning på hvidvask og mifid osv. også selvom man ikke har noget direkte med kunderelationer at gøre. Men det er fint nok.
S	Det er jo meget meget svært det der med at sige hvornår skal vi gemme hvilke data og i hvor lang tid. Bogføringsloven siger 5 år, Mifid siger 7 år, i skærpende tilfælde 8 tror jeg også i nogle tilfælde. Det er sgu svært, det er også en af udfordringer når man skal prøve at lave et setup deromkring, hvordan skal man prøve at tilgå dette på en ensartet måde. Uden at vi skal ind at lave en detail løsninger til den enkelte udfordring.
H	Det der er jo reguleret så meget, at jeg syntes at jeg har set en stor udfordring oppe hos os i hvert fald, ved at det var jo cookie-baseret, med location på for alt det der, der ligger på appsiden, vores beregnere og alt så noget, ikke? Det ligger jo bare der, ikke? Og få lavet nogle retningslinjer for, hvor længe må du gemme det der skidt, ikke?
C	Jo, og hvornår må du samle det op, ikke? Du skal jo have eksplicit consent nu for at opsamle sådan noget.

H	Ja og hvor skal det ligge henne og hvordan får vi det formidlet hvis nu kunden kommer og spørger om det? Altså fordi vi skal jo nok havde *"trykprøve??"* på det, tænker jeg. Af en eller anden sur kunde.
S	Ja, nemlig.
C	25. maj kunne man godt forestille sig at der står en pose kunder der gerne vil teste det.
S	Ja kunder, eller journalister. Det er nok den farligste gruppe [journalister, red.)
a.	Hvad med hensyn til, nu snakkede du jo selv om at implementere nogle processer så I jo ikke selv skal stå manuelt med bolden hver gang. Når det nu kommer til sådan noget som "Right to be Forgotten", er det så noget I har implementeret porcesser direkte om, eller er det stadigt lidt manuelt?
S	Altså som udgangspunkt, hvis vi kigger på right to be forgotten, så er det jo at vi ikke kan finde noget vi ikke har et hjemmel til at holde i vores systemer eller på vores platform i vores bygning, enten om det er elektronisk eller fysisk. Så sålænge vi går ind og siger at vi har sletteprocedure for **alt** i organisationen, så ehh, i vores verden, så findes Right to be Forgotten jo faktisk ikke. Så vores tilgang er mere at vi skal sikre os at vi har sletteprocedurer på **alt.** Så det er implementeret i forretningsgange, politikker, systemer, osv, osv, osv. Så når en kunde kommer og siger at 'Jeg kan se at I har det her data på mig', I ved hvor jeg bor, I ved hvor stort mit lån er, I ved hvad min restgæld er, osv, osv,. Jeg vil gerne have at I slette alt det der". Så kan vi faktisk henfører det til et hjemmel hver gang, og sige: "Jamen, vi vil ikke slette din restgæld, for så ved vi ikke hvor meget du skylder os. " Det kan jo også bare være nogle andre ting vi har lov til at beholde på kunden, fx. hvem han er som kunde, hvad han har betalt, eller hvad han har af indestående - så vi kan levere det videre til det offentlige.
C	Men hvis kunde så stopper med at være kunde, sletter I så alt hvad I har om kunden? Ville I gøre det efterfølgende?
S	Right to be forgotten, og sletteprocedure i det hele taget er jo både på eksisterende og tidligere kunder. Så hvis en kunde stopper med at være kunde nu, så har vi jo bogføringsmæssigt krav på at skulle beholde data'en i 5 år. Så derefter så bliver de jo slettet indenfor de regler der er sat op omkring det. Og det samme hvis det er en kunde

	der handler med investeringer, så er underlagt MFID, så er det en der er underlagt et eller andet område hvor der er en særskilt lovgivning, så gemmer vi det efter den.
C	Så meget af jeres arbejde med GDPR, har også været med at se hvilke steder træder hvilke lovgivninger over og overruler GDPR?
S	Ja og nej. Nu ved jeg ikke hvor meget I kender til IT udvikling?
C + A	Jo, noget fra studiet.
S	Vi gøre vi jo det hele SCRUM / agile setup osv. Og vi har jo lagt opgaverne, hvis vi nu bare tager et eksempel som et system der skal huske og slette. Så har vi jo lagt det ud til Product Owner'ne og sagt: "Det er jeres opgave at vide hvilke data der kommer ind i jeres system, Det er jeres opgave at vide hvilke lovgivninger der er gældende ift. hvilke data de holder. Så vi har skubbet det en lille smule ud, men vi understøtter selvfølgelig hvis de har behov for hjælp ift. de juridiske afklaringer, osv.
A	Nå vi nu snakker om det her med IT systemer, har det så været indkøb af nye IT systemer, eller har det været opdatering af eksisterende systemer? Det lyder lidt som det sidste?
S	Jah. Vi har en meget stor systemplatform. Og så kan vi jo sige at 1. der er sådan systemmæssigt 2-delt i det her. Der er 1 vores eget system platform sådan her nu, eller system landskab med x-antal 100 systemer vi har, som vi skal huske skal ikke skal lagre data lokalt i nogle databaser, eller føre det hen nogle steder hvor vi ikke har styr på data'en. Dem skal vi have opdateret så vi skal have lavet en grad af udvikling på dem. Måske kan vi gøre det ved nogle manuelle slettekørsler, osv.osv osv. Men vi skal i hvert fald havde lavet en eller anden form for opdatering på dem, så vi husker at slette dataen derfra. Så er der den del der hedder at 'Hvordan holder vi så styr på hele GDPR området?' Hvordan laver vi en artikel 30 rapportering hvis datatilsynet kommer på besøg? Og hvordan holder vi bare styr på om vi kan, hvad det er for nogle processer vi håndterer i koncernen? Og der kan man jo have et system, hvor vi ikke har lagt os fast på at købe noget, men vi har lagt os fast på at egenudvikle i første omgang til vi egentligt nemmere kender de krav vi har at skulle styre det op i mod. Så vi måske ikke skulle kigge det på som ' Nu er det kun GDPR vi kigger på', men måske hvordan styre vi hele koncernens, eller organisationsen, risiko-portofolio, ud fra et bestemt værktøj? Der findes jo, nu ved jeg ikke om I kender de værktøj? Men der findes noget der hedder

	Mega, noget der hedder Rismager, og Mega er jo et af de helt store… Det kan alt. Jeg tror der er en finansiel udbyder i landet der har brugt 5 år i landet på at implementere, og stadig ikke har fuldt på plads. Men bruger det super godt, og super aktivt, i forhold til hele deres infrastruktur.
C	Har sådan noget som GDPR, skubbet styring af data frem i forreste rækker? Har det været med til at sætte større fokus på persondata?
H	Det har det i hvert fald oppe hos os, altså i forhold til håndtering af kundedata, altså. Der er det helt klart at nogle har fået øjnene op for at.. Hold da op, puhaa. Og blevet lidt forstrækket over.. Og ikke nødvendigvis det der skal sættes i gang for at lave slettekørsler og registrere og sådan noget. Men bare det at være opmærksom på at sådan noget kan man nu blive spurgt om. Det tror jeg er kommet lidt bag på nogle, for det har jo bare været sådan, fulstændigt… Wild west, ikke?
C	Jo så har man jo bare lige hurtigt sendt en mail til hinanden og så giver man bare lige hurtigt noget information til hinanden.
H	Lige præcis.
S	Jeg tror der er mange som, det er jo det gode ved forordningen, at man personligt kan associere sig med den. Det er jo min og din data som bliver spredt. Hvordan ville jeg have det hvis nogen bare skrev mit personligt CPR nummer rundt i en mail til 10 eller 20 personer. Så selvfølgeligt har det ændret nogles holdning til hvordan vi håndtere persondata, eller personhenførbar data. Det har det helt sikkert. Nu, hvis man kigger sådan, det er ned på hver enkelt medarbejder, og det er jo selvfølgeligt det opdrag der skal være. Kigger vi lidt større, koncern-wise på det, så tror jeg det er noget som er med til at skubbe på en udvikling som mange virksomheder er indeni. Ikke kun vores, men mange større virksomheder. Hvor man finder ud af hvor meget kan man egentligt bruge data til? Altså hvor meget data? Data er guld.
Alle	Ja.
S.	Det er fremtidens guld. Hvordan formår vi at bruge det på en struktureret måde? Det er det her (GDPR) jo også med til at...

H.	Også bare for at få overblikket. Det tror jeg også, for mange har jo siddet med hver sit lille område med sin egen data. For at finde ud af at vi har jo SÅ meget data. Det er jo fuldstændig vanvittigt. Jeg tror aldrig jeg har været et sted hvor man, altså...
S	Vi har mere data end de fleste virksomheder,
H	Ja det har vi godt nok. Det er helt vildt.
S	Og gode data
H	Ja bestemt.
S	Vi skal bare finde ud af at bruge dem på den rigtige måde.
A	Så det har også åbnet lidt op for at kigge på nye muligheder for at anvende denne data på?
H	Ej, der er vi måske ikke kommet til endnu. Men bare erkendelse af at hvor meget data vi har liggende, på mange steder.
S	Jeg vil sige, at det ikke er det der er skelsættende på om vi gør noget eller ikke gør noget. Ift. hvordan vi kigger på data. Det er selvfølgelig noget der er med til at skubbe på, at vi er med til at strukturere det. Men det er ikke det. Det har vi indset tidlgiere. Der skal gøres noget på dette område, hvis vi vil være med. Det kan I vel også mærke (til H.)
H	Ja, der er et helt andet fokus i dag. Alene det, bare navnet på vores afdeling siger alt. Du er nødt til at smelte de 2 afdelinger sammen for at komme nogen steder i dag.
S	Lige præcis.
A	Ja vi har virkeligt set nogle data i dag, hvis vi ser på verden som helhed, der er mange virksomheder der bare lever af det. Altså.
C	Nu omkring den her deadline der er d. 25 maj, vil I mene at I er helt klar til at være compliant til deadlinen? Og i så fald, hvor høj grad er det automatiseret?.
S	Altså, nu sagde du jo selv (til A), ift. hvad er

A	Compliant
S	Ja compliant. HVad er graden af compliance. Ehh. Det vil være lidt naivt at tro at man er 100% compliant. Vi stadig inde og finde ud af hvilket compliance niveau skal vi ligge os på. Og så har vi i hvert fald det meste på plads til den 25 maj, men vi har også noget vi har planer for, hvordan vi kommer på plads med.
H	Ja det er jo også det der er hele keyword'et. At hvis bare du har planen, og du i hvert fald kan dokumentere at du ved at vi vil gøre sådan, så kan det ikke gå helt galt.
A	Det mener jeg også at de har været ude og sige i forbindelse med lovgivningen, at de forventer også at bare at hvis du kan sige at 'Det her er planen og vi regner med at være der på et tidspunkt", så er det ligesom fint nok.
S	Nemlig.
H	Det har vi jo også, i forbindelse med at nogle systemer lukker i forbindelse med de her skæringspunkter, så der vil det være okay at sige at der er noget vi ikke gør på de gamle systemer,
S	Ja for vi udfaser, jeg mener det er 21 systemer til udgangen af det her år. Og skal vi tage en udviklingsomkostning på dem, ift. at vi sagnere dem?
C	Ja det giver ikke mening...
S	Nej, det giver ikke mening. Så der er sådan nogle ting. Og så skal vi jo også finde ud af i hvor stor en grad vil vi systemunderstøtte de processer der bliver håndteret her? Vi kan sagtens øhm, lave en indsigstbekæring, vi kan sagtens lave en portabilitet,.. Men i hvor høj grad skal det være en manuel process af en medarbejder der tager en time, eller skal vi bare kunne trykke på en knap og så ligger det hos kunden 2 sek efter.
C	Og det afhænger vel også af hvor meget efterspørgsel der vil være på sådan nogle ting når det sker ikke?
S	Præcist
A	Nogle af de her kompetencer, nu snakkede du (Hanne) om noget træning, er det noget i har lavet selv internt, eller har i haft fat i konsulenthuse og?

S	Vi har rådført os med forskellige konsulenthuse i forhold til ikke kun at se på dem som en arbejdende hjælp, men i forhold til at trække på deres hjælp og "hvad gør andre" i lignende situationer, så vi et eller andet sted prøver at få inspiration til "what does good look like" på en eller anden måde?
A	Ja, hvad er normen
S	Ja præcist, så har vi prøvet at bruge de her branche organisationer finans danmark til at spare med nogle juridiske afklaringer. hvad ligger de andre spillere med.
C	Så det har også lagt til grund for hvad i selv ville gøre?
S	Ja men nej, ikke så meget at vi lægger et niveau lavere. det gør vi ikke, men vi får ihvertfald en diskussion og en drøftelse om tolkningen af lovgivningen.
C	Ja og det er jo så både med finanstilsynet og andre banker?
S	Nah, ikke finanstilsynet.
C	Jamen er det ikke dem der står for udførslen af GDPR i danmark?
S	Så skulle det være noget helt nyt. Jeg tror hvis du spørger finanstilsynet, om hvor lang tid man skal beholde data, så ville de sige 50 år er godt, 80 år er bedre
Alle	griner
S	og hvis du kan beholde det for evigt så vil det være det bedste. Hvor datatilsynet siger slet slet slet slet. Så der er ihvertfald flere modstridende interesser, om det så ender ud i at det bliver finanstilsynet det tror jeg så ikke det gør. personligt.
C	Ja, men har vi så meget mere?
A	Nej jeg tror at vi har fået svar på de spørgsmål som vi gerne ville have svaret på.
H	Nå, men det var da super. Det var godt du kom (til simon) for der var meget af det der jeg ikke kunne svare på
S	Jah, ja. Så var det godt med en guide til.
C	Må jeg lige spørge om noget follow up?

S	Ja?
C	På et tidspunkt tog i beslutningen til om i skulle opdatere jeres interne systemer eller om i skulle finde en anden udbyder, hvad var de største elementer i jeres beslutning?
S	Hvad tænker du på der?
C	Om i skulle outsource persondata, og opbevaring af denne. Har det været på spil om i skulle finde en alternativ udbyder eller har det været sat meget tidligt i forløbet at det var en opdatering af egne systemer.
H	Har det overhovedet været diskuteret?
S	Nej, (overvejende) Nej det var ikke været diskuteret, vi beholder alt inhouse som udgangspunkt, vi ser ikke et behov for det. Og det er så lidt fint sagt, for vi transformerer faktisk noget af vores master data på vores bank kunder over til en af de her bank centraler BEC. som kommer til at lave en meget stor udvikling på noget af vores system platform. Så det er nemlig også et af de her systemer som vi udfaser ved udgangen af året, det er fordi de ting de varetager de kommer til at blive varetaget af BEC udviklede systemer. Så der kommer til at være noget master data der ligger derovre, men det meste kommer til at ligge hos os. Det er har vi aldrig arbejdet ud fra skulle være anderledes
C	Så tror jeg det var det.

Appendix 8 - Full table of relevant interviewee statements

	Danske Bank	Jyske Bank	Nordea	Nykredit
Size of undertaking	"GDPR has been a major undertaking for Danske Bank, of that there is no question, we have invested a 3 digit million amount in compliance"	"(...) What you always hear from Datatilsynet and other legislative authoratives, is that if you already are compliant, then you won't have a big problem, because GDPR is only a continuation of already existing law. (...) but of course somethings with GDPR are new, and the sanctions are very different."	"I think it would be fair to say it has been a major undertaking, that's not to say there haven't been a lot of legislation previously, but it's apparant that GDPR increases the focus on personal data"	"I would say that the financial sector has had an advantage compared to the other sectors, as we are already heavily regulated. Therefore it doesn't hit us as hard as it might do to others." (...) "(...) this is the first regulation which affects the entire business. Most of the other regulation are department specific, so it is located with a specific group"
Outsourced Competencies	"We haven't outsourced anything"	"We haven't really outsourced competencies, we have had some external legal help (...) We have also had a consultancy help us doing a data flow analysis (...) but that's the biggest place we have had external help."	"We have had a lot of the competencies internally, (...) we have had some consultants to assist as arms and legs, but also for their competencies, but mostly to have some more power in the implementation phase" + "I don't believe that we have made any larger IT implementations due to this [Red. GDPR]" + "We are also in the process of developing a new Core Banking platform, which would have some of the elements that is required"	"We have decided to develop our own solution in the first round".

Considered Outsourcing	"We are a very large player in the market, therefore we can solve most of the problems ourselves"	"We have not" (discussed outsourcing)	"No there hasn't [been any discussion on outsourcing]" "Then I'll think we will hit a more general Outsourcing discussion. As in, how much does one wish to do yourself and how much does one wish to put to outsourcing. And I don't think GDPR breaks anything for us in that discussion." "But that also depends on the size of the company. If we take Denmark, then we see that the local banks, for good reasons, join forces. While, in some different aspects, Nordea and Danske Bank are so big that we are doing some more things ourselves, because we have the critical mass to have the competencies." - Ellen Pløger, Nordea (2018) "The fundamental idea has been to not invent anything new unless absolutely necesarry, instead we would rather update what we have"	

Specificity of Compliance	It is not easy to answer either yes or no to this [specificity of GDPR]. On the one hand there has been some new requirements for, among others, impact analysis, data portability, responsibility of data processors and more. But, at the core, the basic principles for treating personal data, and the requirement for transparency remains at the same level in relation to the data subject. It is merely the consequences of breaking the rules that has been substantially increased	It is not easy to answer either yes or no to this [specificity of GDPR]. On the one hand there has been some new requirements for, among others, impact analysis, data portability, responsibility of data processors and more. But, at the core, the basic principles for treating personal data, and the requirement for transparency remains at the same level in relation to the data subject. It is merely the consequences of breaking the rules that has been substantially increased	I feel that the GDPR legislation are more specific than previous. I'm thinking first and foremost on the demand that we be able to demonstrate that our processes are in compliance with the regulation. At the same time, it is very clear that many may wish that there were clearer description of what is demanded of us. It is in the meantime here, that it is up to the individual organisation to determine what is necessary in relation to 'technical and organisation measures' to protect 'rights and freedom of natural persons' with a background in the organisation you are running."	"The GDPR is clearly more specific than previous legislation in the area of personal data management. The current legislation has, in my opinion, not followed the digital development. So GDPR does, to a higher degree, help organisations with thinking in the right direction. But there is still a large task in interpreting and implementing the new regulation."

Legal changes as a driver of change	"We have also used GDPR as a snowplow, to clean up some things, an organisation that has Danske Banks age and size will naturally have a few messes here and there. As such we have also used GDPR as an excuse to clean up"	We have solutions in place to be, generally, compliant [on the 25th of May]. But I am not completely satisfied with our solutions as is. I know that we have had to chose to use many manuel processes (...) where, eventually, we would like to implement system processes. However, because it is expensive and extensive to make those system changes, and it is not completely known exactly how broad it would become. I mean, if there are 3 persons who would like to use their data-portability during the course of a year, then it is not cost effective to create a solution that costs multiple 100.000 DKK."	"I believe that when new legislation arrives, you always review old processes, and sometimes you find some things that needs to be changed (...) so it is obvious that the increased awareness from GDPR results in actions, also on the technical side"	"GPDR has increased our awareness of the management of customer data" (H) "Many has been surprised, it used to be like the Wild West" (H) "One of the good things about GDPR[in releation to as a driver of change], is that is personally relationable. It is yours and my data that is circulated, and how would I feel, if someone were just passing my personal information around on e-mail to 10 or 20 persons? So clearly it has changed peoples attitude to personal data." (S) "Are we looking a bit broader, on a group level, then I think it has help push us towards a development that many is in (...) and that is that Data is Gold."