The anticipatory quality of organizations towards regulations outlined.
Table of contents

1. INTRODUCTION.......................................................................................................................... 3
2. THEORY .......................................................................................................................................... 7
3. RESEARCH QUESTION .................................................................................................................. 10
4. METHODOLOGY .......................................................................................................................... 12
5. PLANNING..................................................................................................................................... 13
6. LITERATURE .................................................................................................................................. 14
1. Introduction

Nowadays Information Technology (IT) is incorporated in all parts of a person’s life. The presence of IT is facilitated by the rapid technological change since the 1990s (Coffman & Odlyzko, 2002). The establishment of the Internet in particular enables the saving and sharing of (confidential) data online (Sheakh, 2012). Yet, the Internet is lacking appropriate data protection and the amount of cybercrimes is rapidly increasing (Sheakh, 2012). Cybercrimes are often not directly aimed at personal data but provided that most data include privacy sensitive data, almost all cybercrimes concern the privacy of individuals (Saini, Rao & Panda, 2012). For example, WikiLeaks, leaking American government confidential data, was established for the purpose of disclosing original material of powerful institutions for large public (Valeri, 2012). Yet, the leaked documents, for instance informants lists, also contain personal information. Therefore, with the leaking of confidential data, also personal data is leaked (Berghel, 2012; Moore, 2011). Consequently, more thought should be given to the protection of people’s privacy and security on the Internet. Also because privacy is perceived as the greatest concern when using online services (Green, Yang & Judge, 1998; Kobsa, 2007).

The first nation acknowledging the need for personal data protection was Sweden, where the first national data legislation, the Swedish Data Act, was implemented in 1973 (Bennett, 1992:3; Öman, 2004). The aim of this legislation was to protect the privacy of individuals when their data was processed by computers (Öman, 2004). In 1995 the first European Data Directive 95/46/EC was introduced (European Commission, 1995), which additionally incorporates legislation about the free movement of personal data processed by computers (Castro-Edwards, 2013). Member states of the European Union had to introduce the regulations of this directive into their own legislation in order to unify the legislation across the European Union (De Hert & Papakonstantinou, 2012; Fromholz, 2000). This document became the basic reference for data protection worldwide (De Hert & Papakonstantinou, 2012). The implementation of the 1995 European Data Directive has had massive impact as not all Member states were up-to-date with data protection.

Despite the fact that the Internet usage has grown significantly since 1995, the protection of personal information is lagging behind (Saini, Rao & Panda, 2012). With the last major changes in the European regulation of data protection and movement dating back to 1995
(Castro-Edwards, 2013; Triger, 2014), the new General Data Protection Regulation (GDPR) is of utmost importance to extend data protection on the Internet (European Commission, 2012). The GDPR, proposed in 2012 and expected to come into force at the end of 2017 (European Commission, 2012), is focusing on extending the rights of data subjects – the individuals whom the data is about – in the processing and the use of personal data. The GDPR is extending on existing regulations included in the 1995 directive, like: user consent, time limits of data usage, the requirement of documentation, and cross-border transfers (European Commission, 2012).

Yet, with the rapid development of the Internet, new opportunities emerge and new regulations are proposed to adapt to these opportunities (Sheakh, 2012) For instance, the GDPR proposes a ‘right to rectification’ where data subjects have the right to ask for rectification when data is false or incomplete (European Commission, 2013). Additionally, a right to erasure – companies should erase personal data and should do everything to have a third party erase the concerned content – and data breach notification – a company should notify the supervisory authority within 72 hours of a data breach and if feasible within 24 hours – are included in the GDPR (European Commission, 2013). Furthermore, minor changes of the 1995 directive are included in the GDPR. Since the GDPR is a regulation, instead of a directive, it is directly applicable in all member states without changing the national legislation (De Hert & Papakonstantinou, 2012). At the same time, the regulation applies to all organizations holding data about European citizens, in contrast with the 1995 Data Directive which only applied to organizations located in the European Union (European Commission, 1995; European Commission, 2012).

The fact that the legislative power is acknowledging the importance of data protection, emphasizes the importance for organizations to anticipate and be ready to comply to new data protection regulations. Besides, organizations are motivated by multiple reasons to comply to new data protection regulation. Firstly, the way organizations handle consumer privacy is a major indicator of reputation gain or loss (Hirsch, 2013). This is because people highly appreciate their privacy and, as stated, privacy invasion is seen as the highest concern when online services are considered (Green, Yang & Judge, 1998; Kobsa, 2007). Therefore, being seen as privacy-friendly and complying to the data protection legislation is increasing reputation and helps to secure consumer loyalty (Brooks, 2005). Secondly, significant implications exist for organizations violating the data protection regulations. In the European Data Directive of 1995,
organizations could be subject of criminal prosecution when violating the directive (European Commission, 1995). When violating the GDPR, organizations can get a fine up to five percent of their annual worldwide turnover or 100 000 000 EUR, whichever is greater (European Commission, 2013).

As stated, organizations have clear internal as well as external motivations to adjust their organization to new data protection regulations. Hence how can organizations comply to these regulations? The GDPR states that the compliance to the regulation requires appropriate technological and organizational measures (European Commission, 2012). This suggests that multiple departments of an organization are involved when complying to new data protection regulation as is also found in literature (Cook et al., 1983). Complying to new data protection regulation is often considered to concern mostly changes in technology since the data is processed and transferred via IT. Indeed, most articles in the GDPR require new or adjusted technology in order to comply to the regulation (European Commission, 2013). For instance, the right to erasure requires technology that is able to find the right data and erase this data in such a way that it cannot be restored or decrypted (European Commission, 2012).

Yet, changes in technology affect other parts of the organization as well. For instance, when implementing computers, employees have to learn how to work with this new technology. Similarly, the whole structure of the organization has to adjust in order to use the computers in a meaningful way. Consequently, not only technological change but also organizational change will occur when effectively complying to new data protection regulations. These interrelation between departments was already found by Leavitt (1965). Leavitt’s diamond of change (1965) proposes that an organization consist of four interrelated dimensions: technology, task, people and structure (see figure 1). When change in one dimension occurs, the other dimensions react on this change (Leavitt, 1965).
A short introduction: the task dimension focuses on organization supporting activities like processes and what the organization is trying to achieve (Petter, DeLone & McLean, 2013; Thakur, 2013). The people dimension focuses on the employees of the organization and their behavior towards change. Technology include all technology within an organization. And structure indicates the structure of the organizations (e.g. job roles, hierarchy and decision authority). Leavitt (1965) argues that the connection between the four dimensions is critical when successfully changing the organization. Therefore, in order successfully comply to changes in new data protection regulation, all four dimensions are taken into account. When focusing on these four dimensions, new data protection regulations can be complied to efficiently and costs and time can be saved.

With the rapid changing technology, it is expected that more regulations will be established considering data protection. Additionally, since more regulations are established, change in the data protection regulations can occur. In order to be ready for the change in data protection regulation, organizations should be able to effectively comply to new data protection regulations. Following Leavitt (1965), it is argued that the response of organizations to IT change should be an strategy where these four focus areas are balanced. Therefore, a framework will be established for the implementation of new data protection regulations considering the change per dimension and the impact of this change on the other dimensions.

From this the following research question is derived:

_How can organizations adequately respond to new data protection regulations?_
2. Theory

Little is written about how organizations should respond to new data protection regulations. A reason for this can be found in the fact that the last major change in the data protection regulation is dating back to 1995 (Castro-Edwards, 2013). Yet, since the announcement of the GDPR, more and more people are writing about how organizations should respond on this specific data protection regulation, although little scientific literature is available yet (Ashford, 2012; Ashford, 2013; Bunt, 2014; Davis, 2012; Khaki, 2014; Lacroix, 2015). Consequently, the GDPR is used as case study to research how organizations respond to new data protection regulations in general. These responses are mostly focused on the technology side of the organization. According to Leavitt (1965) a change in the technology of an organization also affect changes in other parts of the organization: people, structure and task. However, most of the proposed responses do not take these interconnection into account. Therefore the proposed responses are categorized by dimensions firstly affected.

The major part of the articles in new data protection regulation require technological change within an organization (European Commission, 2013). Consequently, software and hardware costs are seen as the biggest challenge when complying to the GDPR (Network Security, 2015). Technology is therefore assumed to be the core for complying to new data protection regulation which mainly affect the other three dimensions. Accordingly, the most obvious recommendation to comply to the new GDPR is to implement the necessary technology to facilitate the regulation (Khaki, 2014; Lacroix, 2015). Moreover, Lacroix (2015) argues that organizations should implement ‘state-of-the-art’-technology to adequately protect personal data, like the use of encryption.

Although the technology within an organization is assumed to be most affected when complying to new data protection regulation, changes in tasks and processes are of high importance to support the change in other departments and determine the right place for the changes. In order to facilitate the right place for changes, organizations should understand their data life cycle, to know where what information is processed (Khaki, 2014, Rubin, 2013). When organizations have a clear understanding of the data life cycle, they can implement the required processes in the right place (Khaki, 2014). Moreover, organizations should know what data they
process and should assess the risks of this processing in order to know the responsibilities the organizations has (Rubin, 2013). Consequently, organizations should consider which information actually needs to be stored and all irrelevant information should be destroyed. This provides a clear overview of the important data (Culkin, 2015; Rubin, 2015). For instance, with the ‘right to access and obtain data’ proposed by the GDPR, organizations should at every moment in time be able to give data subjects information about what data of theirs is being processed (European Commission, 2013). Moreover, processes should be put in place to log and monitor every time someone accesses the data (Rubin, 2015). This documentation provides the organizations with an overview of who has access to which data and when this data is consulted. This is necessary for accountability and to detect security breaches as early as possible (Rubin, 2015). Lastly, the necessary security policies should be implemented to meet all privacy requirements and the necessary processes should be put in place to comply to the new data protection regulation (Rubin, 2013).

Changes in processes and technology also affect changes in structure. Additionally, when complying to new data protection regulation, structure can significantly change. For instance, the GDPR proposes that organizations employing 250 persons or more should appoint a data protection officer (DPO) who supervises the data protection within the organization (European Commission, 2013). Moreover, even when no DPO is required, it is recommended to assign ownership for the required changes when complying to new data protection regulation (Culkin, 2015; Rubin, 2015). It is important to have someone responsible for the compliance to new data protection, especially because the fines for violation of regulations are very high (Culkin, 2015).

It is considered that most changes occur within the technology dimensions when complying to new data regulations, however when implementing IT systems, behavioral problems are more likely to occur than technological problems (Ginzberg, 1978). It is therefore of high importance to consider the employees when implementing new information technology. When the employees do not see the purpose or meaning of the change, people will have no incentives to comply with this change (Ginzberg, 1978). Engaging the employees in the change will avoid this problem (Khaki, 2014). Moreover, it is also of high importance to make sure the employees are trustworthy and integer, to avoid unnecessary data breaches via employees (Lacroix, 2015). Additionally, to decrease the risk of data leakages, limited access should be
given to employees, only the employees who work with the personal data should be able to access the data (Rubin, 2015).

From the literature a first draft of the framework can be established:

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Actions</th>
</tr>
</thead>
</table>
| Technology | Implement necessary technology for compliance  
              Implement state-of-the-art technology |
| Task      | Implement necessary processes for compliance  
              Implement necessary policies  
              Understand data life cycle  
              Delete irrelevant information  
              Know what you are processing  
              Document of data access  
              Assess risks |
| Structure | Implement necessary structure changes  
              Assign ownership |
| People    | Engage people  
              Make sure employees are trustworthy and are integer  
              Limit the access of data |
3. Research question

New data protection regulations require adjustments to the existing data protection measures within an organization. Although, different organizations often take comparable measures to comply to new data protection regulations, no general guideline exist. A guideline of such could significantly help organizations to comply to new data protection regulations in an efficient manner and could save time as well as costs. Hence, this research focuses on the establishment of a framework that organizations can consult when complying to new data protection regulations.

From this the following research question is derived

How can organizations adequately respond to new data protection regulations?

Firstly the existing data protection measures within an organization are taken into account, to allow cross-organization comparison of data protection. Therefore the first sub question is stated as:

1. What measures are already implemented for data protection?

In order to review which data protection adjustments are made when new data protection regulations are implemented, the GDPR is taken into account. The GDPR is the first major change in data protection regulation since 1995, hence significant changes are incorporated within this document. Therefore, the changes within the GDPR are assumed to be representative for general changes within the data protection domain. Data protection experts of different organizations are interviewed about their measures taken to comply to the GDPR. From this the second sub question is derived.

2. What measures should organizations take in order to comply to the GDPR?

As stated in the GDPR, the supervisory authorities are allowed to establish new data protection regulations or make changes to existing data protection regulation on basis of specific cases (European Commission, 2013). This and the fast changing technology indicate that changes in data protection regulation are likely to happen. Therefore, the data protection regulation framework that will be established will focus on complying to general data protection measures. Considering the measures already implemented and measures that should be taken for the GDPR, it is reviewed which measures should be taken into account when new changes in data protection regulation occur. From this the third sub question is derived.
3. What measures taken for data protection are generally applicable when a change in data protection regulation occurs?

When establishing the framework Leavitt’s diamond of change (1965) is taken into account. Leavitt argues that the four dimensions: technology, task, structure and people are interrelated and a change in one dimension cause changes in the other dimensions. Keeping this in mind, measures for new data protection regulations are categorized by these four dimensions and the influence of these measures are taken into account in order to keep the balance within an organization. From this the last sub question derives.

4. How can Leavitt’s diamond of change be used to categorize and extend the (influence of) measures taken for data protection?

From this a draft of the data protection regulation framework will be established. Evaluation of the framework will take place by the same data protection experts as interviewed. According to this evaluation, the framework will be improved and a final version of the framework will be established.
4. Methodology

In order to carry out this research, first literature review will be conducted on existing literature about responses of organizations to new data protection regulation. A first draft of the framework will be established from this literature gathered.

Thereafter, data protection experts are questioned about the response of organizations to new data protection regulation. The first draft of the framework is discussed and input is asked for changes in the framework. Additionally, input for the interviews will be gathered.

Following, a semi-structured interview will be conducted with data experts of organizations that are subject to the GDPR. A semi-structured interview provides the advantage of having a guideline for taking the interviews, but leaves space for extra questions and in-depth interviewing. The data experts will be questioned about their strategy towards the data protection regulation, and which approach they use considering the four dimensions. Here, the GDPR is taken as a case for the compliance to new data protection regulations in general.

The interviews conducted will be interpreted via coding. A code scheme will be established and every interview will be coded according to this scheme. This will categorize the data and provides a clear overview from which results can be easily derived.

From these results a general framework is established as a guide for organizations when facing the implementation of new data protection regulations. The framework established will consider Leavitt’s diamond of change concerning the following four dimensions: technology, task, people, and strategy. General approaches for responding to new data protection regulation are included in the framework. From this the final draft of the framework will be established. Hereafter, a focus group will be established in order to evaluate this draft data protection regulation framework. When possible, the same data experts as interviewed are asked to evaluate the framework and pose improvements for the framework. From this the data protection regulation framework will be established which will lead to discussion and conclusion of this research.
5. Planning

The table below illustrates the planning of this thesis.

<table>
<thead>
<tr>
<th>When</th>
<th>Tasks</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>April</td>
<td>Literature review</td>
<td>Introduction / theory</td>
</tr>
<tr>
<td>April</td>
<td>Gather participants</td>
<td>Participants</td>
</tr>
<tr>
<td>April</td>
<td>Set up interviews</td>
<td>Interview set up</td>
</tr>
<tr>
<td>May</td>
<td>Conduct interviews</td>
<td>Data</td>
</tr>
<tr>
<td>May</td>
<td>Start processing interviews</td>
<td>Results</td>
</tr>
<tr>
<td>June</td>
<td>Process interviews</td>
<td>Results</td>
</tr>
<tr>
<td>June</td>
<td>Focus Group</td>
<td>Results</td>
</tr>
<tr>
<td>June / July</td>
<td>Analyze results</td>
<td>Discussion and conclusion</td>
</tr>
</tbody>
</table>
6. Literature

2015, from: http://www.computerweekly.com/feature/Do-not-delay-EU-data-protection-
changes-on-the-way.

from: http://www.computerweekly.com/news/2240178256/How-will-EU-cybersecurity-
directive-affect-business.

Bennett, C. J. (1992). Regulating privacy: data protection and public policy in Europe and the


Brooks, G. (2005). Keeping customers' personal data safe is good for business. New Media Age,
18.

April 16 2015 from: http://www.marqit.nl/newsitem/13024

Internet Law, 17(3), 3-8.

Telecommunications IV B: Systems and Impairments, IP Kaminow and T. Li, eds, 17-56.

Thesis Design


