the LISBON MBA
católica | nova

Title:	The Impact of the Data Protection Officer (DPO) in the Firm's Strategic Decisions
Field of study:	Corporate Governance
Purpose:	Dissertation for obtaining the Degree of Master's in Business Administration
Author:	Pedro Guerra Alves
Thesis Supervisor:	**Professor Doutor Duarte Pitta Ferraz**
Date:	11 July 2019

ABSTRACT

This dissertation adopts an exploratory empirical research method in order to address a subject that has recently gained considerable media and corporate attention. The urgent focus on the issue in relation to the principles of data protection in corporate governance and the business world results from the fact that although the General Data Protection Regulation (GDPR) affects virtually all companies and requires them to employ a data protection officer (DPO), in fact, the reality does not reflect this. Of the almost 27 million companies in the European Union required by law to enforce GDPR regulation, most have never heard of their requirement to employ a DPO in full compliance with the legislation, even though full observance of GDPR became mandatory as of 25 May 2018.

The current research analyses the role of the DPO and explores its potential to impact on the business world. The research assesses the transformational effect the GDPR paradigm has had on the system of corporate responsibility of the businesses that must observe it. In particular the competencies and responsibility bestowed on the DPO when effectively it gave the role the power to take responsibility for and actively influence the direction of a company's strategic decision-making.

In order to identify the gaps, the research commences with an examination of the nature of this transformational paradigm, focusing on its origin, development and finally its execution. The analysis then focuses on the selection, appointment and profile of the DPO and additionally gains insight into the role, actions taken, and structural implementation of the DPO role within organizations. Examination of the relationship of the DPO with other stakeholders and its relationship with the board produced pertinent data, allowing the researcher to come to a number of conclusions as to the impact of GDPR, the DPO's role, and the role's relevance to corporate governance.

This qualitative research, using semi-structured interviews, selected interviewees according to the criteria adopted, with focus on organizational reputation and the importance of personal data-handling. The DPOs were selected from multinational listed companies operating in data-driven sectors (e.g. banking, telecommunications, pharmaceuticals and retail) because, as these organizations deal with massively sensitive data as an indispensable part of their core business, the DPOs within them play a pivotal role in terms of influence.

What emerged from the research is that the involvement of the DPO differs: sometimes the DPO is central to the development of GDPR compliance and sometimes the role is there just to ensure compliance and provide training. The research suggests that the DPO does has real influence at board level; however, the hypothesis is also that the DPO can directly intervene in the decision-making processes of organizations, either in the development or in the execution of GDPR, as a direct result of their involvement in the implementation of the strategy.

Finally, even though GDPR is a very recent paradigm, which means there are no guidelines or case laws to refer to, this does not diminish corporate responsibility to comply. However, as businesses often rely upon instinct and community, and base practice on trial and error, the consequences – both positive and negative – are yet to manifest.

Acknowledgements

I would like to take this opportunity to express my indebtedness to everyone who in one way or another has made it possible for me to complete this Master's dissertation. Only with a favourable combination of many uncontrollable factors did the opportunity arise for me to undertake studying for my Master's and writing my dissertation.

To me, the chance to contribute to the academic community is a privilege representing a space for personal reflection, investigation and expression of freedom of thought, and coming with the unique responsibility to educate my fellow citizens and add value to the intellectual capital of society.

I cannot offer enough words of appreciation to Professor Duarte Pitta Ferraz, to whom I pay simple homage by thanking him wholeheartedly for the precious and profound knowledge that he bequeathed to my cohort in the field of Corporate Governance. I must also offer special gratitude to him for agreeing to supervise my dissertation and for maintaining a constant readiness to welcome and assist me, never failing to respond to any request I might make.

I would like to express my gratitude for the support of my colleagues at Alves & Associados: without their empathy, assistance and expertise undertaking this research would not have been possible.

I would like to thank the interviewees for their availability and 'transparency' and for trusting me with their statements, without them this academic research would not have been possible.

To Mandi for reading and recommending changes to the dissertation, ensuring that mistakes made by the student, whose first language is not English, were corrected to allow the Supervisors and Examiners a smoother reading.

I would like to thank Nova School of Business and Economics and the Católica Lisbon School of Business & Economics for their unique and immeasurable partnership and the creation of the Lisbon MBA Program, and extend special thanks to everyone who made this possible.

Finally, I must thank the fundamental pillars that have held up and balanced me while studying for my Master's degree: my parents and sister and my friends. A special thanks to Adriana for her affection and sacrifice while living dedicated to this project, for her constant and unconditional support, as well as for her stimulating, always enlightened analytical approach to the theme.

Abbreviations

APEC CBPR Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System

BCRs Binding Corporate Rules.

CCEPC Communication from the Commission to the European Parliament and the Council – Commission guidance on the direct application of the General Data Protection Regulation

DCGK Deutscher Corporate Governance Kodex (Regierungskommissiion)

DPO Data Protection Officer

EBA European Banking Authority

ECIIA European Confederation of Institutes of Internal Auditing ECIIA – European Confederation of Institutes of Internal Auditing

EDPB European Data Protection Board

ENISA European Union Agency for Network and Information Security

EU European Union

FERMA Federation of European Risk Management Associations

F&P Fit and Proper Regime

GDPR General Data Protection Regulation - Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016

HEDPL Handbook on European Data Protection Law

IAPP International Association of Privacy Professionals

IFC International Finance Corporation

IPCG Institute for Portuguese Corporate Governance

IT Information Technology

OECD Organisation for Economic Co-operation and Development

OECD-PF OECD Privacy Framework of 11 July 2013

The Charter Charter of Fundamental Rights of the European Union

WP29 Article 29 Data Protection Working Party – Guidelines on Data Protection Officers ("DPOs")

Table of Contents

1 Synopsis of the Thesis: The Data Protection Officer and Corporate Governance

Over the last few decades the world has seen unprecedented technological and economic growth. Powered by innovative, complex business models, the relationship between communication and IT are renowned; and geographic borders meanwhile have become merely dotted lines on a map. Personal information has evolved into a valuable commodity; it is used to crucial competitive advantage (Porter, 1980) by both corporations and governments, while research and academia are struggling to keep up. It is undeniable that while use of data can yield great societal and economic benefits, the consequences to citizens' rights to privacy, and other such rights, poses a threat to society: "the abundance and persistence of personal data have elevated the risks to individuals' privacy" (OECD, 2013).

Personal data protection emerges as a secondary concern because it has the potential to detrimentally affect economic growth and hinder innovation. This reality is visible currently in corporate governance. Fostered by evolving partnerships and new techniques to take advantage of data, the lack of responsibility taken by organizations, voluntarily, in relation to the protection and/or abuse of personal data, had become noticeably unacceptably poor. The future of data is uncertain if, as Moore's Law (1965) holds, the expectation is that the amount of data stored and transacted will continue to double about every two years in unexpected ways. The current dissertation examines the concerns around what purposes data can serve, the nature of which undoubtedly is set to change greatly over the next few years. Therefore, the data that corporations store for undefined purposes to use later, to either gain or maintain a competitive advantage, and the consequences it may have for sustainability and reputational risk, are relevant.

Trust and accountability, inevitably, are crucial preoccupations for all stakeholders. While there are several regulations and guidelines available to corporations, the EU's General Data Protection Regulation – commonly referred to as GDPR (approved on 27 April 2016; effective from 25 May 2018) – imposed a set of procedures, the effects of which have been felt most keenly within the business community, which demand a change in mentality. GDPR "forced" companies not only to understand the regulatory framework that would require them to adapt their technological systems, organizational models and processes, but also to comply with it. Ultimately, GDPR changed the paradigm from hetero-regulation to mandatory regulation with the "privacy by default" rules (WP29, 2018). This means that corporations are now responsible for inception of compliance with GDPR regulation, including employing and developing the role of the Data Protection Officer (DPO). However, the corporate governance currently in place is not yet fully prepared to assimilate the paradigm shift.

The current dissertation focuses on the future of data protection in the business world and in wider society, with the objective, in the words of the European Parliament and of the Council (2016), that "the processing of personal data should be designed to serve mankind".

2 Research Methodology, Method, Conceptual Framework and Ethics

The research methodology and methods chosen to develop this research have taken a pragmatic realist approach. A methodology first developed by Charles Sanders Peirce (1839–1914), Duarte Pitta Ferraz (2012) also adopted it for the purposes of his research. In essence, pragmatism takes the stance that fixed and external standards do not determine "truth", but rather that truth emerges from a process of interpretation (Mounce, 1997). Peirce presents a structure for the idea of abduction, treating it as a precursor to deduction and induction, as a way to create "scientific knowledge". Abduction is associated with the utilization of knowledge to identify the potential cause of a problem (Fisher, 2007).

Pragmatism draws attention to the philosophical views that constitute traditions, this in order to identify what is actually being claimed when certain properties emerge and are advocated (El-Hania, 2002); while realism is a philosophical theory, partly metaphysical and partly empirical, which can be tested by experience but often goes beyond it (Leplin, 1984). Rescher (2000) develops an argument for pragmatic realism by advocating that the main objective of science is to present a model of reality that is useful, and stresses that realism represents a presupposition of inquiry. Pragmatism in the main is characterized by the relationship between theory and praxis, these sharing a common interpretation of truth, complemented by their relationship in practice (Ferraz, 2012).

Applied fields have made use of qualitative-data research only since the 1980s, including in business studies, where the shift generally has been more towards the qualitative paradigm (Ferraz, 2012). Qualitative data then became a source of enlightening information, made up of rich explanations of undeniable quality, obtained from interviews and organized into convincing incidents or stories, supported by a conceptual framework (Miles, 1994). Pragmatism puts emphasis on practice and discourse, rendering meaningless any discussion about the reality independent of human theories and conceptualizations; pragmatism, therefore, provides a philosophical framework to support a "realist interpretation" of reality (El-Hania, 2002).

The current research uses the data from semi-structured interviews of Data Protection Officers from multinational listed companies as its central method. The decision to interview a number of elites was, as Bellamy (2011) observes, due to the interviewees' relationship specifically to the area of the research. Complimenting this method were bibliographical analysis, secondary data and qualitative research data to identify opportunities and gaps. Particular emphasis is on multinational companies, with a strong presence in the Portuguese economy, maybe using a diversity of corporate governance rules and decision-making processes.

The interviews acquired special relevance in this dissertation, since the research explores a recent reality for which there is limited secondary data and academic research available to explore. From a social science perspective, John Dewey (1859–1952) also stressed the importance of the connection between theory and practice by taking a social and a community-based view of "theory and knowledge". Theory should be tested by acting upon it, he advocates, and its truth, or otherwise, will emerge through the development of a social consensus. This is perhaps the core of pragmatism: there are no definitive or authoritative ways of determining truth; rather, what is true is that which is of use (Ferraz, 2012). In

gathering the statements of the interviewees, while their views were limited to their respective sectors and experiences as DPOs, their insights were not replicable. Learning of their knowledge and expertise, their particular interests and involvement made a valuable contribution to the research. Nonetheless, their assessments represented in some cases the "politically correct" (Florence, 2015) point of view, due to internal influences and their professional responsibilities and ambitions. Hence, it was felt that the pragmatic-realist methodology was the most appropriate way to produce results suitable to the characteristics and objectives of the research (Ferraz, 2012), and thus this is why the researcher adopted a pragmatic-realist qualitative research methodology.

3 Corporate Governance and the Role of the Data Protection Officer

There is great political interest in the role of the DPO in corporate governance, induced by market globalization, weakened entry barriers and aspirations to take the competitive advantage. The EU and other nations have the utmost interest in protecting a valuable commodity such as data (WP29, 2018).

The critical literature review, which initially employed Hart's (1999) methodology to source the relevant literature, has since been updated and reviewed to identify the connections between themes, theories and the current research according to the research objectives – that is, to identify the impact of the DPO's role in listed multinational firms' strategic decision-making processes. Thus, this section analyses the multidisciplinary relationship between the reciprocal obligations of governance and the DPO. Furthermore, this section explores the questions pertaining to the obligation of organizations to appoint a DPO, the benefits and the difficulties, and observation of how the DPO fits both into the current corporate governance models and into the relevant concepts of corporate governance—that is, the concepts developed by the Cadbury Committee (1991) and IFC (2017, 2015).

A transformation of corporate mentality is required in order to respond effectively and compliantly to the change in paradigm, which largely redefines privacy, and introduces new functions and importance to the role of the DPO. This redefinition is still in its first year and therefore has not yet brought any noticeable change, while any response from or improvements to corporate governance are not yet apparent either. Inevitably, the business world will take time to adapt to the innovations presented by GDPR and, in particular, to realize the DPO's impact on corporate governance and the "Defence model" put forward by FERMA/ECIIA (2006), which is comparable to what already happens with other important functions such as auditors and accountants.

Detailed analysis of the regime that regulates the DPO and the role's impact on corporate governance are both vital in order to understand the DPO's influence over the decision-making processes of corporations. Further analysis of whether the DPO can either directly or indirectly block or promote certain strategic decisions is also necessary, in order to see if this influence over decision-making results from the responsibilities bestowed on the postholder by the EU. These responsibilities bestowed on the DPO by the EU include an obligation for the postholder to formally inform the board and supervisory authorities of breaches. At the same time, however, the role of the DPO has been given protection by various principles, which means that the postholder cannot be penalized or dismissed for any reason in relation to the performance of their duties (GDPR, 2016). The current research utilizes the business-

strategy perspective developed by Michael Porter (1996) in order to analyse the question of how the DPO intervenes in the definition stage of a strategy and whether this effects the subsequent allocation of scarce resources, capital and human resources.

The role of the DPO acquires particular relevance in terms of the future of corporate governance, especially as the introduction of the role came about as part of the “privacy by design” standard within organizations and that appointing someone to the role is compulsory (WP29, 2018). Inevitably, therefore, corporate governance (models) must adapt to this new reality (GDPR, 2016). Historically, the purpose of corporate governance was to look after the interests of shareholders, but according to several economists, now “most authors define the question of corporate governance as the means by which shareholders control the board of directors” (Lenoble, 2003). A recent shift to meet the interests of all stakeholders (IPCG, 2018) means that the DPO’s role will inevitably influence this objective. This is an understanding mirrored by both the German Corporate Governance Code (2017) and the UK Corporate Governance Code (2018). As data is an increasingly valuable commodity, essential to the future prosperity of organizations, it is therefore essential that all businesses should take responsibility and invest in their systems of accountability and competences to “ensure the continued existence of the company and its sustainable value and its sustainable value creation” (DCGK, 2017). Designed specifically to assist such sustainability, the guidelines state that the DPO’s role in data protection should be transparent (HEDPL, 2018), which is achievable by implementation and update of the corporate structure, codes of conduct and corporate guidelines. Thus, as the subjects and gaps need to be identified in order for the theory and practical conclusions to emerge, Figure 1 (Relationships and Subjects), below, illustrates the intrinsic relationships and subjects pertaining to good corporate governance.

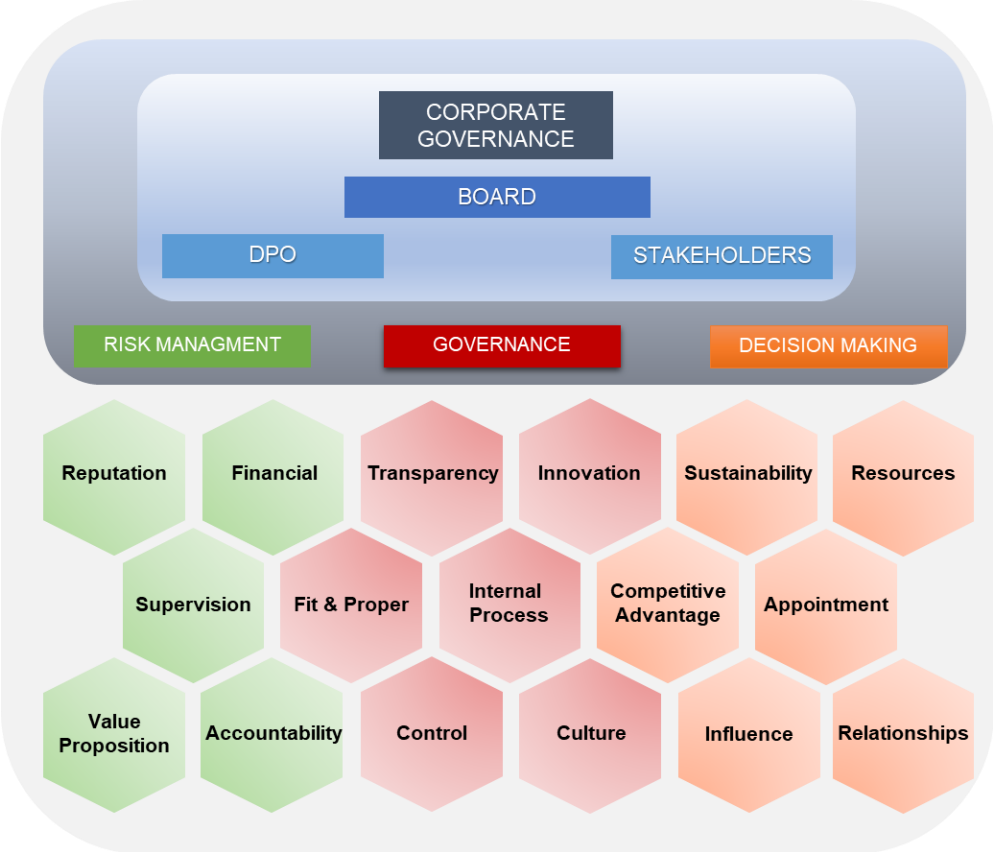

Figure 1: Relationships and Subjects

3.1 History and evolution of the role of DPO in corporate governance

Privacy and data protection are ancient concepts, but the reality surrounding them has changed dramatically in the last century. From the emergence of automatic-computerized processing, to limitless data-storage capabilities, to the instant recording of events (photography and video), to the "post-industrial revolution" (Bell, 1973), data has always been a valuable commodity. While data is of growing economic value, organizations and governments often retain large amounts of personal data for a number of purposes. Invariably, as with anything of value, security, protection and misappropriation are relevant subjects (IAPP, 2018a).

Historically, the European Convention of Human Rights of 4 November 1950 was the first major step, elevating privacy to a fundamental human right: "The protection of natural persons in relation to the processing of personal data is a fundamental right" (The Charter, 2000). The International Covenant on Civil and Political Rights (United Nations, 19 December 1966) followed. Thenceforth, privacy-protection become a global concern, with many of the world's organizations conducting studies and introducing regulation and guidelines. Of particular importance among these are the work developed by the European Union's system of Binding Corporate Rules, the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System, and the OECD. The OECD actively participates in protecting economic development and any negative impact data might have on the global economy, especially among OECD members. The first major development came with the OECD's "Privacy Guidelines" in 1980, reviewed in 2013 to meet the "changing technologies, markets and user behaviour, and the growing importance of digital identities" (OECD-PF, 2013). The EU continues to develop important regulations and directives, with their first key development with regard to personal privacy the Directive 95/46/EC of the European Parliament, followed by that of the Council. With the Treaty of Lisbon in December 2009, the EU elevated the right to privacy to the status of a separate fundamental right (The Charter, 2000). More recently, the EU substituted the Directive 95/46/EC with GDPR (approved 27 April 2016, with effect of 25 May 2018), which adapted the fundamental right in order for it to meet the current and future reality, with mandatory and direct application to all member states.

GDPR has revolutionized the way that organizations should seek to protect data, demanding a different corporate mentality and introducing two new principles, of data protection by design and data protection by default. Furthermore, GDPR introduced another substantial change in the regulation, changing it from a system of notification to a principle of accountability. Essentially this means that now both corporations and governments are responsible for the conception of an internal data-handling policy to protect people's data, with heavy consequences for mishandling said data – in other words, for not complying with GDPR. At the same time, GDPR elevated the role of the DPO (from the previous Directive 95/46/EC), increasing the DPO's responsibility and accountability and making the appointment of a DPO mandatory for many corporations and business sectors, including in all the public services and religious institutions. EU member states are currently busy developing GDPR policy, whose development, implementation, and monitoring the EU left in the hands of individual nations' and organizations' internal regulatory systems themselves to implement use of the guidelines. This includes creating or updating supervisory authorities and the development of administrative, civil commercial and criminal procedures,

legislation, codes of conduct, as well as the recruitment of a DPO to meet the mandatory appointment of someone in this role in all public services. Thus, while the main concern of the EU's regulation is the protection of a fundamental human right to privacy, the objective, however, is to assure such protection is forthcoming, while at the same time safeguarding the freedoms of the EU so as not to limit economic growth or innovation (GDPR, 2016).

The fundamental ideas behind data protection have always been a secondary concern to corporations and governments alike, although the concept has always had an elevated status (OCDE, 2013). The reason behind this may very well be the fact that data is not yet easily taxable; and similarly, that the role of the DPO is a recent one, introduced less than 30 years ago. The role of the DPO has attracted plenty of attention since GDPR came into effect (25 May 2018), yet studies, guidelines and recommendations regarding its specific function are limited, and in some areas non-existent. In short, with such great importance given to data protection recently, inevitably, the world's leading organizations must comply and thus corporate governance must also reflect this recent reality (OCDE, 2013).

3.2 The obligations of corporations: Appointment and profile of a DPO

This section looks at appointment of the DPO from the perspective of the corporation and the intrinsic complexity that establishing the role poses. Appointing a DPO is an additional compliance responsibility rather than an obligation, with the responsibility for the appointment of the DPO falling entirely on the corporation (GDPR, 2016). From the perspective of corporations, therefore, it represents an additional cost without any immediate return. Even though this was never the intention behind the idea of the DPO appointment, the grievance is partially true however, at least in the short-term. Nonetheless, the expectation is that, long-term, the DPO role will benefit corporate culture and improve the value proposition of and for corporations (CCEPC, 2018).

The rules pertaining to the hiring of the DPO leave a wide margin for manoeuvre with regard to competences, expertise, skills and ability (CCEPC, 2018). This is understandable, however, if you consider the millions of corporations in the EU and the different corporate governance models in effect among those millions and then those of the separate member states as well. While there are no clear obligatory competencies that the DPO needs to possess as such, with regard to educational background, certification, degree, or minimum experience, it is compulsory that the DPO's appointment reflects the complexity, volume and, most importantly, sensitivity of the data and related issues that arise within the organization (GDPR, 2016). There are qualifications that a DPO candidate needs to have, such as "expert knowledge of data protection law and practices" (GDPR, 2016), and the postholder should own management and communication skills to better deal with the management/board, internal staff and supervisory authorities. In addition, the DPO should have management-level experience in cyber security, risk and compliance, as well as knowledge of organizational IT infrastructures, business models and governance (CCEPC, 2018).

Well-known is that the recruitment and hiring of the DPO is a complex process with an inherent high-level risk (WP29, 2018). The risk arises from the fact that it is the responsibility of the organization to demonstrate and justify its choice of DPO; an inept choice of DPO is a valid reason for non-compliance

(CCEPC, 2018). In essence, the board appoints the DPO, and the DPO should report directly to the board, yet the DPO is not answerable to the board but to the data protection laws. Penalizing or dismissing the DPO for any reason in relation to performing his or her role is a breach of GDPR. In addition, in order to comply, the DPO must have free access to virtually all departments and processes (HEDPL, 2918), which presents an additional difficulty in terms of implementation.

3.3 Appointment: Considerations and parameters

By default, historically, compliance with data protection has been in the hands of IT managers or the chief data officer (HEDPL, 2018). The intention of GDPR is not to undermine the jobs these personnel do to protect data in any way; for, according to GDPR, the role of the DPO fills a specific gap in data-protection compliance, which concerns the protection of the individual rather than the business. Therefore, the limits and incompatibilities between the DPO and other roles happen to relate to and overlap with the jobs of the self-same IT managers or chief data officers (IAPP, 2018a) with whom responsibility for data protection has historically been placed.

When corporations go about appointing a DPO they must take into account multiple considerations, and must define the parameters for the position founded on two fundamental concepts: the principle of independence and the existence of conflicts of interest (GDPR, 2016). There are other relevant considerations that must be taken into account to support the appointment of the DPO, including the parameters of the job within the organization and the level of skill enumerated according to the different regulations, guidelines and national legislation. Some such parameters are: time-availability, resources, competence and organizational relevance, expertise in risk and IT evaluation, credibility and assurance that there is no conflict of interest; independence and confidentiality, legal expertise, cultural and global awareness and having the “common touch”, leadership and project-management skills, and board-level relationship management, (HEDPL, 2918).

Looking at this from the business perspective, another relevant competency is of the utmost interest: the DPO should also have knowledge and experience of the organization’s trade, products/services and market. Essentially, this should include knowledge about how the organization earns its revenue, the strategies in place and the resources at hand (IAPP, 2018b).

This extensive list of requirements is fundamental at two levels: first, in order for corporations and prospective DPO applicants to verify that their qualifications and experience fulfils the main requisites of the post. Second, that the DPO is able, as part of his or her function, to validate if the corporation is complying with GPDR (WP29, 2018), which includes the choice of DPO, and therefore means that the DPO must check if she or he fulfils the necessary skills and competences to perform the DPO function. This vast set of requirements will no doubt evolve over time as corporations put them into practice, learning from their own and others good practices as well as mistakes.

3.3.1. Responsibility and accountability of the DPO and corporation

Responsibility and accountability are the cornerstones of data protection, and by extension are therefore the main requisites of the role of DPO (GDPR, 2016). These acquire particular importance when examining the current hypothesis, as both are essential to determining whether the DPO can or cannot

intervene in decisions that have bearing on data protection. These two different interconnected and dependent concepts (WP29, 2018) need analysing from two different perspectives – both the perspective of the corporation and from the DPO's viewpoint. From the perspective of corporations, organizations are subject to the fines established by GDPR as well as liable to pay compensation to any offended parties. In contrast, the DPO is not directly responsible for paying either the fines or compensation. Nevertheless, GDPR (WP29, 2018) leaves the question of the DPO's personal liability wide open. Such a possibility is a paramount concern, for not only does it increase risk in terms of the DPO's performance in carrying out the role, but it also limits the ability of the DPO to perform the role's intended objectives.

Deepening the complexity of the issue still further: while the responsibilities of the DPO lay primarily in assuring the protection of personal data, as the person responsible, the DPO must also do everything in his or her power to ensure compliance. Nevertheless, limits to this objective lie not only in the company's ability to provide the DPO with the necessary resources, but also to give free access to all areas of the organization in order to perform the DPO function, including in sensitive areas and in highly confidential matters (GDPR, 2016). As to the DPO's responsibility in situations where there is a breach, for the first such event the responsibility may only fall on the person/entity who committed the breach, but there seems to be some consent that when breach events are repeated the DPO will be held responsible under civil, administrative or criminal law (WP29, 2016) as well. Therefore, the inference is that it is in the DPO's best interests when confronted with recurring scenarios to act immediately to avoid them, doing so either through the complaints procedure or, if required, to intervene by shaping decisions, as this dissertation hypothesizes.

With regard to the accountability of the DPO, in recent years, due in large part to the high number of data-breaches and many mediatic cases, "the principle of accountability received renewed attention as a means to promote and define organizational responsibility for privacy protection" (OECD, 2004). There are many important principles regarding data protection that the laws and regulations legitimize. Nonetheless, there is a crucial one among these for the DPO; this is the accountability principle, whereby the DPO is a "cornerstone of this principle of accountability" (WP29, 2016). All the other principles are unworkable without the existence and implementation of the accountability principle. The accountability principle states simply that the DPO is accountable for complying with the measures that are effective to the principles regarding data protection (OECD, 2004). Therefore, the question arises: if the accountability of the DPO is limited to this extent, then how can she or he intervene or influence decisions? As stated above, the research recognizes that the DPO holds limited liability according to GDPR for the consequences of strategies and decisions put in practice by the board. However, with the professional integrity of the DPO at stake, with his or her responsibilities bestowed by the board, inevitably the DPO is going to feel directly accountable for any decisions and, therefore, feel that actively intervening is in his or her own best interests.

3.3.2. The independence principle and conflict of interest

While the accountability principle (GDPR, 2016) regulates the "accountability" of acts, the independence principle regulates the DPO's ability to exercise such acts; that is, to fulfil the role of the job. As the DPO

is responsible for a variety of tasks, the independence principle is in place to ensure that the DPO can perform his or her function, even though the DPO may be responsible for several public authorities and bodies (OECD, 2018). Nevertheless, applying it to corporate culture is a highly complex and challenging task to accomplish. It is made especially complicated by the fact that the DPO can perform other tasks and have other contractual obligations. This becomes the more salient when considering that the DPO can be held responsible if she or he does not fulfil the obligations of the role (HEDPL, 2918), while in contrast, employees, contractors and management may not be held responsible for incompetent or negligent decisions in this way in their day-to-day jobs.

These principles work in partnership with the obligation of the DPO to abide by the secrecy and confidentiality rules that apply to their role (WP29, 2018). Secrecy and confidentiality are of special relevance to the role of the DPO and are essential to him or her carrying out his or her duties effectively. However, it is difficult to comprehend the real scope and practical execution of the role in this regard, for the research suggests that there are significant obstacles in the implementation of this cornerstone principle (OECD, 2013). One of these obstacles deserves detailed examination, as it is a relevant indicator to measure the DPO's influence at board level. Compliance with legislation around secrecy and confidentiality are fundamental responsibilities in some professions (i.e. for lawyers, medics and priests) (IAPP, 2018a). However, while these responsibilities in professions such as these are essential, the result of years of study and certification, in the case of a DPO, the same responsibilities simply result from an appointment from a corporation. Currently, the academic framework and appropriate certification to provide the trust factor to a profession such as the DPO does not exist, which raises the question as to how and where the DPO will gain the trust and the reputational respect the role demands (IAPP, 2018a).

Finally, supplementing the principle of independence are the rules relating to limiting any conflict of interest in the performance of the DPO's duties (GDPR, 2016), especially since the DPO can fulfil a number of other related tasks and duties (OECD, 2013). Nonetheless, the task of ensuring that no conflict of interest interferes in successful implementation of the role of the DPO lies in the hands of the corporation and the DPO. Furthermore, corporations (in a case-by-case way) can develop internal guidelines and identify incompatible positions, but even with the extensive list of principles and rules still it is challenging for any employee or subcontractor to place the responsibilities that come with the role of DPO (IAPP, 2018b) above his or her own personal professional aspirations.

3.4 Who fits the DPO profile? A problem for corporate governance

The question of what makes the ideal DPO profile has particular relevance in the field of corporate governance, and this is the subject of this section of the dissertation. The research demonstrates that this question of DPO profile, which is still in the early stages of development, is causing uncertainty in the business community because there is no conclusive answer. The researcher seeks to answer the question "Who fits the DPO profile?" This is a three-pronged question, which reflects the complexity of the role: asking whether as currently regulated, the DPO can gain or be shown to already have the necessary competencies; whether the role influences board-level decisions; and whether shareholders, the board and stakeholders can trust that the person appointed has the correct capabilities and influence

to perform their duties. Therefore, this question, “Who fits the DPO profile?” (IAPP, 2018c), is of significant importance.

Consider the following aspects of the role of the DPO: the DPO is responsible to apprise and advise the board, senior management, his or her team, and employees generally, essentiality every part of the corporation. The DPO is also responsible for monitoring compliance, raising awareness and general and specific training, reporting to the auditors and supervisory authorities, as well as performing an active role by intervening in the day-to-day business of the organization (GDPR, 2016). Furthermore, the DPO must have extensive legal and IT expertise, which are two areas that in general do not develop together either at an academic or professional level. Thus, subsequently this mismatch, between desired competencies professionally and the educational resources or workplace training to facilitate the role, creates a shortage of qualified personnel, implying that several companies will be experiencing and will continue to experience difficulties recruiting an experienced DPO (HEDPL, 2918). Therefore, the scope of the role of DPO – the safeguarding of stakeholders’ interests – and the DPO’s position and responsibilities within an organization, directly affect the rules of corporate governance, which must adapt, assimilate and outline the function in accordance with the law. Additionally, the number of qualified DPOs globally in the next few years are expected to reach 75,000 (IAPP, 2018c), but this is a small number in comparison to the corporations currently operational, thus a potential skills shortage is generating yet another obstacle.

As inferred, readying organizations to meet all the requirements of GDPR presents challenges. Compounding this is a lack of transparency (illustrated in Figures 2a,p. 20 and 2b p. 28) whereby the owner of the data (the individual) has no direct control over the choice of a DPO or voice to challenge the decision, and thus, without having access to the postholder personally, there must be an implicit trust that the DPO employed is suitably qualified. Other obstacles arise in addition, such as enforcement, as this varies according to jurisdiction and, thus, inevitably, there are the leaner and less effective authorities (WP29, 2018). Taking Portugal as an example, as this aspect of compliance was one of the gaps the research highlighted, three years after approval of GDPR Portugal has yet to implement the mandatory regulation and procedures of it. This has resulted in a deficiency of resources, infrastructure and enforcement (EDPD, 2019). In addition to the various principles and mandatory rules listed by the GDPR guidelines, there are the mandatory rules and principles of corporate governance that are already in place. Thus, while a practical implementation of both regimes is required, the current research shows that this has created a complex and expensive challenge for corporations, because without concrete and consistent guidance on implementation of GDPR, multiple governance systems have been adopted in relation to the choice of and implementation of the DPO role (Figure 4, p. 41). This lack of standardization reflects negatively on the internal rules of corporate governance, which is an effect identified as a gap in the current research. Thus, while acknowledging that there is no one option that all companies should adopt, still the research suggests that the existence of dozens of potential solutions to comply with GDPR cannot benefit stakeholders’ interests.

From the perspective of academic research and the business world this situation creates an interesting gap, especially considering that the guiding principles of corporate governance put “trust and

transparency" (OECD, 2016) at the top of the list. To comply with the extensive requisites and rules imposed by GDPR and simultaneously to provide stakeholders' assurance that they can trust the DPO, certification, a multi-task team, and a Fit and Proper (F&P) regime seem to provide possible solutions, these are hypothesised immediately below in the current research to overcome this gap.

First is the DPO's certification. A solution to the matter is already being developed by the Spanish data protection agency (Agencia Española de Protección de Datos, 2018), which appears to be a viable solution, with greater feasibility, and especially advantageous for small and medium size corporations. Second is another solution that is best suited to multinational companies that do not tend to handle highly sensitive data. This involves the appointment of, or outsourcing to, a DPO multi-operational team composed of lawyers, IT and other professional specialized in the specific business sector. Third is a solution of utmost interest to corporate governance. This solution is directed especially at sectors with a large stake in society and the world economy, and where data is of fundamental importance to the core business. This option would suit organizations such as those operating in the financial, pharmaceutical, IT and social media sectors, where it is suggested that they should adopt a system of rules analogous to the F&P regime that is currently in force within the banking and financial sectors.

There are many similarities between the principles and skills required for compliance with GDPR and the F&P regime (Ferraz & Castro, 2018), thus looking to F&P could benefit the appointment of DPOs. The intention behind the creation of the F&P regime was that it would act as a gate-keeping function for credit institutions and investment firms, both to safeguard their composition, appointment and succession policies and the qualifications of the management body, i.e. on the board of directors, key individuals and representatives. The evaluation of the F&P regime resulted from a need to correct the management deficiencies identified in the governance of banks, which led to excessive management risk taking and allowed inadequate compensation practices (Ferraz & Nannicini, 2018). The F&P regime is now compulsory for the appointment of members to the management bodies of significant credit institutions that fall under the direct supervision of the European Central Bank. Examples of the relevant similarities between F&P regime and GDPR are the political and economic objectives (Basel Committee, 1999), which are there to help rebuild the public's trust in the financial sector and to restore the sector's reputation, as well as to improve the security and soundness of individual Institutions (Ferraz & Nannicini, 2018). Another similarity with GDPR is the F&P regime's purpose as a prevention and supervision tool, whereby its role is also to assess continually individuals' ability to make sound, objective and independent decisions and judgements, directly in order to safeguard and protect the company's reputation. Furthermore, the purpose of the F&P regime (EBA, 2017) is to guarantee, through assessment of its different criteria, that the management body has adequate expertise, competence and independence; furthermore, that they are able to commit sufficient time and effort to accomplish their responsibilities effectively, and that there is no conflict of interest. Collectively, the F&P criteria plays a crucial role in assuring that the management body has adequate qualifications, expertise and experience relevant to each of the material activities of the institution, and that it has a full understanding of the nature of the business and its risks (EBA, 2017). Other similarities exist with regard to rights to access, conflicts of interest and independence of mind – thus, according to the F&P regime, if the member has other jobs or professional interests that may collide with the functions of their post, for example, being

on the board of a computing company, this might inhibit the individual's suitability. Another is the time commitment – according to the F&P rules the member must demonstrate that he or she has the time to develop the functions and responsibilities attributed. Ultimately, the aim of the F&P regime is to improve financial culture, and to develop managers who are capable of making "good profit" decisions in order to build sustainable organizations (Ferraz & Nannicini, 2018).

As the many similarities between both requisites are also common in most legal regimes governing the selection of positions of public-private interest, it would seem advantageous to take the positive elements of the F&P regime and implement them in GDPR. These positive elements, alongside the motivation to make this comparison, is due mainly to the possible inclusion of the fitness and propriety tests of the F&P regime when making DPO appointments (EBA, 2017). The fitness test evaluates the individual's expertise and competence to fulfil their responsibilities. Competence is evaluated using evidence of formal qualifications, previous experience and record of accomplishments. The propriety tests assess the individual's integrity and suitability (Basel Committee, 1999). The adoption of a similar test for the appointment of DPOs appears to be a measure that could benefit both corporations and the EU's efforts to protect personal data, not only by helping shore up compliance but also by harmonizing the regulation. Notwithstanding, while a certification regime might prove to be more advantageous with less risk attached, this route would represent a higher cost for corporations and individuals and thus could potentially affect the revenue of governments. In contrast, GDPR and EDPD (2019) have instituted and developed an accreditation system for the certification bodies of the supervisory and regulatory institutions of each country. This could either demonstrate a lack of confidence in the current institutions ability to supervise these areas, or could express recognition that there is a clear institutional gap, reflected in the corporations also, which comes in the shape of a distinct lack of qualified personnel to enable full compliance with GDPR (EDPD, 2018).

To conclude this section on the F&P regime's relevance to GDPR, it is clear that a solution is needed to mitigate the issues and gaps identified in relation to GDPR. It is also clear that there is a need to demand that corporate governance is based on the recruitment of "fit" leaders who own the ability to manage the rapidly evolving, transnational institutions that seem increasingly intangible by geographic dispersion (Ferraz & Nannicini, 2018). Thus, a significant component in the future selection of DPOs may be to implement "transparent selection processes that includes effective mechanisms of identification of potential candidates and […] for nomination, proposals for election or co-option, those with the highest merit" (IPGG, 2016), as already exists for the selection of board members in many jurisdictions.

3.5 The DPO transition to Corporate Governance

This final section, bearing in mind the discussion above, examines how introduction of the DPO can improve corporate governance. The very positioning of the DPO within an organization already provides insight into whether and how the DPO intervenes in decisions and how much the role influences the organization's decision-making, or whether the impact of the DPO on the decision-making processes of the organization is minimal. Therefore, it is necessary to define the introduction of the DPO in corporate governance, which can be understood either by looking at the appointment process or by observing the level of responsibility and/or positioning of the DPO within an organization. Undeniably, the figure of the

DPO assumes a role with an elevated status and influence, such that non-introduction of a DPO may have a perverse and negative effect on the organization in the long term. Therefore, the hypothesis is that the positioning of the DPO in relation to internal governance and its functions should make use of the “lines of defence model” developed by the FERMA/ECIIA.

Using the “lines of defence model” as the foundation, the objective of which is to protect all stakeholders, shareholders and the board, the model succinctly states that corporations have three independent control functions or lines of defence, these are internal audit, risk and compliance (FERMA/ECIIA, 2916). According to the analysis of the interviews, the DPO exercises all three functions, with special emphasis on the compliance function (EDPD, 2018). Nonetheless, while seeking to enforce the principles of independence, conflict of interest, and the extensive list of mandated tasks, the DPO cannot be placed within the compliance department or any other similar department, or be controlled directly by senior management, because the DPO is mandated directly by the board. The situation becomes even more complicated, however, since the DPO cannot be a former or current employee of any of these departments, bar the full-time allocation of personnel holding senior positions in those departments. As such, the question arises: how will organizations (re)structure their corporate governance structure to enable the DPO to exercise an independent compliance control function?

Three theoretical positions of the DPO with organizations have been hypothesized as Figure 4 (p. 30) illustrates, although none is optimal for all types of organizations. Therefore, a case-by-case evaluation founded on complexity and size would seem the most appropriate measure. Positioning the DPO at senior management level (Figure 4a, p. 31) is a solution that seems to be in line with the aims of GDPR. In addition, a fourth line of defence (Figure 4b, p. 31) was implemented in the figure of an external DPO (similar to the position of an external auditor) (Figure 4c, p. 31). Interestingly, the research concludes that companies currently position the DPO in the organization across all of the hypothesized positions and, thus, there is no obvious most popular place to position the DPO. Why this has come about is not clear, it could simply be down to choice, or could mean that companies are still uncertain about where best to place the DPO within the organization.

The DPO’s position in an organization is currently exclusively a board decision, and as all organizations seem to insert the DPO in different positions within the organizational set-up according to their own preferences, there is no concrete conclusion as to which suits the role’s aims better. However, as most DPOs have only been in practice for a short period, one could assume that organizations are still adapting and defining their internal governance. The position as outlined by the organization, besides the internal rules implemented, inevitably defines the DPO’s influence within the organization. Internal-governance assessments should monitor how the DPO influences and interacts with the board and the other departments and whether the DPO is directly involved in the decision-making process of the board, either by offering guidance or formally providing opinions, or whether the DPO is involved only at a later stage with the development and implementation of strategies. Both propositions allow for speculation about the real value of the DPO in a firm’s strategic decision-making processes.

4 Qualitative Research: Interviewees, Gaps, and Research Conclusions

Following the review of the literature, this section will describe the interview process, collection of data and examination of the discursive material. It will draw conclusions by analysing the semi-structured interviews and qualitative research in order to elucidate the hypothesis presented above. More specifically, focus in this respect will fall on whether the DPO does have a direct or indirect influence over an organization's strategic decision-making processes. In addition, this section will provide the profiles of the interviewees selected for the research and the criteria implemented for their selection.

All the interviewees approached are currently DPOs practicing in multinational listed companies with a large presence in Portugal. These companies are operating in the finance, fintech and pharmaceutical sectors. All of the interviewees own knowledge of their organization's sector and GDPR policy and have a breadth of experience in performing the job, with the potential to produce and expose pertinent research results. The researcher recorded the interviews and took notes. He transcribed the interviews from the notes and recordings and translated the same into English. The division of the questionnaire reflected the topic and the gap that was being explored. Each of the interviewees signed a confidentiality agreement. As the interviews adopted the principle of confidentiality and anonymity, the interviewees remain anonymous by using pseudonyms, yet with unidentifiable profiles to indicate their responsibilities, type of organization and their position, whether an internal or external DPO.

The questionnaire was organized into three parts: framework-introduction, core-development and conclusion. The framework-introduction focused on the appointment and implementation of the DPO. The core-development section focused on the relationship and power-dynamic with the different players – the board, employees and stakeholders. Finally, the interviews concluded with a discussion based on facts about the role of the DPO in the strategic decision-making process.

Analysis of the recorded interviews began by listening back and selecting the most relevant statements to emerge from the interviews. Then these statements were organized according to topic, gap, and interviewee. The narrative was constructed by weaving in the relevant material from the research according to gap and topic, to part-fill the gaps, and then weaving in the viewpoints expressed by the interviewees. Conclusions were drawn according to gap and topic, and a global conclusion, emerging from the research, allowed recommendations to develop in order to bridge the research gaps identified.

4.1 Framework-introduction: obligations, impact, appointment and profile of the DPO

Identifying the main changes brought about by GDPR and by the elevation of the DPO's importance, the interviewees referred to the transformation of mentality or mindset their organizations were undergoing as the foremost improvement, as mentioned by Richard R.: "*The model has completely changed; the company is totally responsible for what it does. Whatever you do is your responsibility. The DPO appears as an advisor*, *holding the flag. At one time or another it is consciousness*; *it is the cricket of companies.*" Other organizations took up the momentum and went a step further *"[...] reflecting on the processes, revisiting the processes, not only to comply with the law, but to make them more efficient"*, for which they needed to "*be very reactive at this initial stage and for the next few years."* (Francis C.) There was identification of numerous obstacles with reference to the complexity of the

administrative process, which now is seen as the only way to implement this new mentality, in particular: "*Virtually every company member was involved, some with more responsibility and others with less."* (Richard R.) Similarly, Francis C. describes the process as being far more complex that initially thought: *"It is an area in which it is difficult to give people autonomy."* Additional difficulties brought about by hiring subcontractors was seen by Albert C. saw as the biggest challenge and risk: "*We pass data to companies, but how can we ensure that these companies comply with the rules? The management of subcontractors is one of the biggest challenges facing the organization. How do we control this risk? How do we control the chain of subcontractors?"* As expected, the risk of hefty fines and penalties is a constant preoccupation. Nonetheless, organizations adapted to it and assimilated it as another business risk, *"Personal data, is personal data, and we need it to work and grow sales, etc."* (Richard R.), which makes it clear that many organizations will continue to work with data because they must do so, despite the risk, and even when mandated on the limits.

Not surprisingly, organizations woke up late to the reality of GDPR. When the interviewees were asked about how they came to take up the position of DPO and respectively about the recruitment process, Albert C., for example, stated: *"The company needed someone who knew the internal processes, who could do something in a short time."* According to Richard R. the DPO appointment was filled in line with an internal fulfilment of requirements more than with any evident recruitment process: *"The conclusion was that it was better to appoint an internal person."* Many of the internal candidates had no substantial prior knowledge of GDPR or what the DPO function entailed, or went through a formal recruitment process, as exemplified by the comment by Alvaro C.: *"There was no recruitment process. It was a very natural step*." In fact, as the more common practice was by invitation of a board member, it might be deduced that the main requirements were prior experience with supervisory and regulatory procedures, in house influence and/or knowledge of IT.

Theoretically, two professions emerge as best suited to the role of DPO: lawyers and certified information systems auditors (CISA), this is according to Thomas J. Shaw (2018). However, this was not evident from either the interviews or the research. First, none of the interviewees had those backgrounds; and secondly, the interviewees offered valid arguments to explain the reasons behind why a legal background (lawyer) was unsuitable. Even so, the interviewees highlighted the fact that it was essential to have a lawyer and/or an IT specialist on hand to directly support the DPO. Inevitably, all professions were seen to have their own advantages and disadvantages in relation to the ideal background of the DPO. Although, there is no specific GDPR-related rule that the DPO must come from a legal background, many skills that are necessary to the role of DPO point to it as a suitable professional qualification. However, it is essential the DPO have both legal as well as IT knowledge as part of an in-depth understanding of GDPR. In addition, the research makes clear that the DPO should be a well-respected person with in-house experience, who knows the company culture and politics, and that the role should have the support of a team including lawyers and IT personnel (Shaw, 2018).

The interviewees inferred that a considerable gap exists in the recruitment procedure in place for hiring the DPO. Thus, while there is targeted or even excessive preoccupation by organizations initially in the first year, the lack of a proper recruitment process to fill the post of DPO, either by GDPR or internal

corporate governance, may create favourable scenarios for future exploitation and/or neglect. For example, a number of authors already refer to the occurrence of auditors willing to bend the compliance rules "a bit" as a "*shop for compliant auditors*" (deFond, 2018), so could the same happen with the role of the DPO — i.e. a "shop for compliant DPOs"?

Describing their experience, the interviewees explained their methodology and actions in their role as DPO. The role of DPO *"[…] is a function that can be very ungrateful, I recognize the importance of it, the added value is a very large paradigm change, but if it goes wrong it can create many antibodies."* (Francis C.). Others saw it from a more business-oriented perspective: *"The role of the DPO is to help innovate in the solutions, the formulas and processes we have in place to sustain growth; it is the opportunity to grow more and innovate to improve customer experience, retention and consumption and increase our share.*" (Richard R.) From an external DPO perspective, Bernard S. described his experience differently: "*Our work has become more technical in the execution"*; and classification of the role as a service provider means *"there has been a lot of compliance work and awareness that the data must have an impact across the organization",* using a direct approach. He continues that here has been "*a lot of action to bring the company to understand issues about the problems of personal data."*

Following the change of mentality, what value does the DPO bring to an organization? The amplitude of responses varied greatly, conditional on the reputation, background and involvement of the postholder. Interviewees inferred that the responsibility bestowed on them by the board was of utmost significance, and, as such, the value direction tended to a business-oriented value proposition. In such a direction, Bernard S. mentioned: "*This is not so much a matter of fines, but a question of added value for companies, how companies can handle the data, and especially in their relationship with the various players in the market*." Moreover, from his perspective: *"The processing of data – as external DPO – the concern is that the treatment must be done from the perspective of what in terms of business and strategy is right without question."* (Bernard S.) This was a view complemented by Albert C., who focused on an additional imperative subject, that of reputational damage: "*[...] more important than fines is the reputational damage brought by non-compliance."* Overall, the answers came to the same conclusion: that the DPO "*protects the business and the company, naturally."* (Francis C.) Clearly, there is a need to reconcile business and data protection, as Richard R. outlines: "*We must be smarter, we must find alternative ways*, *but they are not so cheap, it all costs money. The implementation has high costs*"; the same interviewee provided another insight in relation to the potential value of the DPO by referring to the role's access to customer complaints: "*From the inbound customers we learn what they complain about; what they complain about provides input from which we have managed to extract rich information*."

Organizations, businesses, corporations, they all figured out the value of data a long time ago, and consumers are only beginning to see the damage its unregulated use can inflict upon them. While there are many value propositions the DPO can offer to corporations, nonetheless, the business-oriented DPO stance reveals a gap – a mismatch between the value-proposition for the citizen/consumer against that of the organization. Not one of the interviewees identified this issue. It could be concluded, therefore, that such value is achievable only by constant pressure from external stakeholders (consumers,

regulation and supervision), which so far has been virtually non-existent. According to Figures 3 (p. 31), there have been three official fines, (based on the information made available by European Commission at 25 May of 2019), from among 136,682 complaints and data breaches across all of the 28 EU member states, with the largest relates to Google (Alphabet Inc.) for 50 million euros, which represents 0.006 per cent of their 820-billion-dollar stock market value, whereas the other two were below 20,000 euros (see Figure 3d, p. 31). While, more recently, in July 2019, the UK Information Commissioner's Office, as emitted two record breaking fines for the lack of security in a data breach, to British Airways and Marriot Hotel Group, for 183M£ and 100M£ each.

The interviewees were asked to identify or summarize some of their experiences as the DPO role rose in importance. Francis C. described her experience: "*It was a year of some indecision with companies very wary of large fines, and this meant that they did things that maybe they did not have to do*"; adding a small criticism that "*Not even citizens want that level of protection.*" In the pharmaceutical sector, Michelle P. put forward a different argument: "*This is an already ultra-regulated business [...] because we deal with very sensitive information. Did I notice differences? No. We were already careful.*" Richard R., meanwhile, described his experience: "*GDPR at the limits wears the hat that represents the customer experience. We need to transform our customers into promoters of our service and not into detractors*." The overriding consensus is that there must be an adaptation to this new mindset, and such adaptation must start from the top and filter down through the organization. Bernard S. elucidates this point: *"It is not easy for the DPO, in companies where the administration is not very involved, to be able to bring about a change in the mentality or strategy. It will always be dependent; and there is an increased degree of external DPOs that may not even* really *exist, or certainly not be as accentuated as internal DPOs*." Nevertheless, even without due institutional support and even with the lack of historical cases and guidelines, DPOs performed their role using common sense and by supporting each other: "*There is no doctrine. There are many new things that we do not know where to go with them*." (Albert C.) Similarly, "*This is all live and learn.*" (Richard R.) In short: "*Having a DPO makes sense because we are living in a different world; we are actors in a world where access to information has to become more civilized.*" (Michelle P.)

There is still a great deal of non-definition in relation to both the role and value of the DPO. Motivating this lack of definition are internal factors, such as uncertainty about the value of the role and its position in the organization, and external factors, such as the lack of orientation and definition by the supervisory entities. To validate this point, Bulgaria, Czechia, Greece, Portugal and Slovenia are the only five EU member states that have still not yet adapted the mandatory national laws in relation to GDPR, which were approved three years ago. The conclusion to draw here is that non-definition and lack of supervision could devalue the role of the DPO.

4.2 Core-development: Relationships and the power-dynamic among the different players

Relationships, with the different players and stakeholders, and the DPO's position within the organizational structure was a subject that held particular importance. Bernard S. began: *"Regulation is more than a law as it brings added value to the relationship with all the various stakeholders."* The process must begin by identifying all the players, *"[...] which we call Privacy Champions [...] who are*

responsible for building the interface between the players and the organism that is somehow managing this." (Richard R.) Subsequently, recognition of the obstacles such as the timeframe and consideration of the organization's size are essential: *"The path is difficult in a large organization, but it is necessary that every organization realizes that things have changed. Currently, this degree of alertness exists only in areas of criticism. This must be everyone's topic." (Richard R.).* On the subject of getting employees to comply: "*There were people, especially in marketing, who were opposed to what we wanted to do."* (Albert C.). Thus, focus fell on efforts to promote a new employee mindset: *"In relation to all areas of the company the idea that customer privacy has to be by default was pursued, impacting everything, to change our thinking and how we develop products, systems, processes, etc. […] and therefore this was not always easy."* (Richard R.) This was a view complemented by Albert C.: *"One of the themes for this year is the degree of sensitivity/awareness of the Company."* Changing the mentality of the board was another objective that falls within the DPO's role, "*It is very hard work in this first phase to pull the administration itself towards this theme*." (Bernard S.) This is a stance highlighted by Albert C., who was of the view that it all starts with the board "*They must be sensitized; it must happen from top to bottom."* Albert C continues by talking about how culture change must involve the practical involvement of all departments and subcontractors: *"One of our daily activities that has more weight are requests for advice on many internal drives, with special focus on the most innovative areas*." Inquiring about the DPO's relationship with the board, the responses were quite similar, describing a monthly reporting relationship with the board member responsible: Richard R. said: "*I report to an administrator, with whom I have a monthly meeting [...] where I report on the last month [...]. Typically it is a quick meeting."* He continues that there are also semi-annual meetings with the board, which are "*Larger Meetings with the board, typically one or two a year whenever there are events that justify them."* (Richard R.) Also mentioned was evidence of the direct relationship with the DPO and a named board member, in part as a function to facilitate a fast mechanism of action in case of an emergency (i.e. a data breach).

The case with external DPOs presents an altogether different relationship. In this contractual role, DPOs are viewed as service providers who provide training and external consulting, as stated by Bernard S., who stated that he communicates "*With the board or with contact points. And if necessary, we will have to communicate directly with the board."* The same interviewee also suggests there is a noticeable difference in the execution: "*We are present once a month for a week, for two or three days, we raise awareness, review processes and analyse issues.*" This presents a less personal and involved function that may well prove to be less influential than the in-house DPO.

The relationship between the DPO and the board requires further examination of the DPO's position within the organizational structure. As the DPO's role only recently came into existence, preparation for its introduction within organizations has been slow catching up. Thus the role, and its position within organizations needed creating from scratch, as mentioned by Albert C.: *"One of the themes was that the whole body of internal governance was non-existent as was the normative body to provide a set of rules and internal procedures, so the company had to make use of internal practices. You must have a model of government that works and a team that works with processes and practice*." While GDPR guidelines do provide guidance, the reality is recurrently different – whether this is for practical reasons, cost or corporate interest. Francis C. defines the situation: *"Initially, at the time, a DPO was 100%*

desirable – there was a lot of work to do." Richard R. echoes some of the other interviewees, describing *"a somewhat stand-alone role, reporting directly to the executive committee, but without a direct team. There was an outside consulting team in connection with the legal and auditing and risk management areas."* (Richard R.) Others stated that the DPO's role was created *"as a multidisciplinary team within the company to provide the DPO service."* (Bernard S.) Albert C. stated that the DPO's role "*has the structure of a bank, operating within the organization, and giving instructions to it, actively intervening within the business."* All in all the result has been that each organization has been opting for a different operational structure, which, in terms of structure, has resulted in the DPO being supported by either an external or internal team, with legal and technical support. Sometimes the creation of quality- and data-management departments were already partially in progress and then the DPO improved them once in post. In some cases, the DPO was directly involved in the process of launching new products rather than brought in as an advisor at the final stages, as Albert C. states: *"[…] the role of the DPO is to create scenarios, or respond to scenarios, and identify risks."* Organizations delegate a variety of functions to the DPO, dependent on their prior competencies, in some cases with *"[…] direct operational involvement within the company."* (Richard R.) Other DPOs, such as in the case of an external DPO, stated: *"The DPO's role is understood more from the perspective of assessment and recommendations […]; as external people we do not intervene much."* (Bernard S)

Delving deeper into the issue at hand, two other topics were discussed: firstly, the potential for a conflict of interest and the independent principle, and secondly the DPO's accountability. The rationale behind this line of questioning relates to how the DPO can perform the role's functions, while avoiding a conflict of interest and maintaining independence, if the role is business oriented, accumulates two functions, and when, inevitably, the postholder's contract is with the organization. As one of the interviewees stated, since the DPO is still an employee this presents a problem: "*The position was instigated because the DPO is dedicated to performing the functions of the role, but part of the time the DPO has to be dedicated to the company."* (Michelle P.) Getting more directly to the point, Francis C. stated that if the role has *"two functions, one will be left behind."* Furthermore, there was the question of how the DPO's role can influence practice if the DPO is not responsible for his or her decisions; as one interviewee suggested, *"[…] fortunately the DPO is free from risk.*" (Richard R.).

This last statement is particularly concerning. However, none of the interviewees suggested that they were irresponsible when going about their job; rather the opposite was true, as they enumerated a list of functions including the risk, responsibilities and decisions they took in their role as DPO. However, there is a clear gap in the mentality of the DPO and the real function of the role. It seems unrealistic for the DPO, or any professional role, to come with relevant responsibilities and be an active part in decision-making process, without the individual accepting responsibility and accountability. Both the independence and lack of accountability of the DPO is incompatible with the current importance of the position and responsibility bestowed on it by the GDPR, and organizations' dependence on the role in terms of corporate risk. While the role may appear feasible in theory, nonetheless, it appears not to be enforceable.

There are two important reasons why examining the DPO–board relationship is worthwhile. First, to understand the level of responsibility the board confers to its DPO. This was something called out by Richard R.: *"People understand that the DPO is an important figure, and the fact that the law requires the DPO to report to the administration gives it also ascendance and power for the rest of the organization to respect, and this is very important."* Second, is the nature of the role the DPO plays within the board: is she or he an auditor, advisor, lawyer, supervisor, employee, business partner or a service provider? The suggestion from among the interviewees was that there is no clear role for the DPO: each organization conceived their own image of the DPO role, influenced more by the person appointed than the regulation itself. The person chosen for the post of DPO reflects the importance given to the role by organizations. The more influential, experienced and widely known, the greater the influence and power the DPO has on the structure of the organization and the board, resulting in recommendations that have more influence to block or promote a certain strategy.

To conclude on this subject area, the relationship between the DPO and the board develops naturally enough as normally seen in this sort of hierarchical relationship. However, one of the gaps in the DPO's function is the protection bestowed on the role. For example, while the DPO's function is to advise and inform, if the circumstances demand, the DPO might have no choice but to submit a complaint to the supervisory board. Furthermore, the protection mechanisms in place (i.e. the DPO cannot be penalised or dismissed), are unrealistic, for anyone who performs admirably all the DPO functions under GDPR, but costs the organization a multi-million euro fine, say, will inevitably suffer the consequences. Therefore, there is little benefit for the person performing the DPO function to do so compliantly.

The competencies of the DPO are more relevant than initially predicted. This is because organizations developed their DPO post around the proficiencies of the person appointed initially. Granted, this strategy may prove to be effective, but nonetheless it raises the question of how the consumer can trust the DPO appointed. To answer this question, 50 listed companies were analysed (see Figures 2a (below) and 2b, p. 28) from the perspective of a consumer (following the rules mandated by GDPR).

Listed market		**Type of DPO Designation**		**Identification of the DPO**	
CAC 40	6	No clear designation	15	Identifiable physical person	2
DAX 30	7	Direct designation	2	No information	15
Dow Jones	9	Privacy department	33	Generic contacts	33
IBEX 35	10				
PSI 20	18				
Internal/Outsourced		**DPO Requirement: Based on Complexity Risk**		**Area**	
Internal	35	Imperative	38	Energy	3
No clear information	15	Medium	3	Financial	20
		Low	8	Hotels	1
				Industrial	6
				Pharmaceutical	5
				Retail	6
				Technological	8
Total number of listed corporations analysed = 50					

Figure 2a: Results of the findings of the informational research into DPOs in listed corporations (from Figure 2b, p. 28)

An initial search took place for DPOs via the published (official) websites of organizations and then a search-engine search followed. Secondly, a brief examination of the characteristics of the DPO

appointed was conducted, alongside the position of the DPO in the company's structure (internal or external), using information publicly available, such as the biography on the organization's website. From the 50 listed companies, a prior classification was made, based on the sector, to define the DPO's obligations – classified as imperative (39), medium (8), and low (8). The results were surprising, as Figure 2a (p. 20) and Figure 2b (p. 28) demonstrate, showing that only in two companies, both of which were banks, was it possible to identify the DPO appointed by name. Of the others, 15 published no information and 33 published generic information. Furthermore, most companies chose to employ an internal DPO (35) – a conclusion reached based on the type of contacts available – while of the other 15 it was not possible to classify. These numbers are staggering considering that most of these organizations deal with highly sensitive and valuable data, that they are all part of complex business groups, and that transparency and identification of the DPO are the very cornerstones of GDPR.

As suggested, the lack of transparency is a relevant gap from which several concerns arise, and yet the interviewees were unable to provide a logical explanation for this scenario of unidentifiable DPOs. To overcome this the Fit and Proper (F&T) regime may serve as a solution, for several reasons. The DPO is a function that comes with an extreme level of responsibility and vast requirements in terms of competence, yet the responsibility for compliance and consequences for not filling the role with the best candidate is the responsibility of the organizations themselves. Research of the market suggests that this scenario does not happen in any other relevant or mandatory functions. For example, take certified accountants, auditors or lawyers, they all need certification, and in the case of board members in banking they also need approval. No other legal or regulatory position has been identified that does not require some type of certification or approval. This suggests, therefore, that not imposing the same level of scrutiny to the role of the DPO, which, as stressed already, is essential to the protection of the fundamental rights of all citizens, is the first step on a dangerous path for the future. Nonetheless, the interviewees identified many problems with implementation of F&P (or certification) categorization: *"There are not many people in Portugal who have the capacity to perform the DPO function alone [...] one person alone cannot own all the necessary competencies."* (Bernard S.) Furthermore, the same interviewee drew attention to the fact that small-and medium-size organizations *"[…] do not have the capacity to create internal teams that can support the DPO."* The same interviewee went further to state: *"Certification will result in a professional who will be high cost, but guarantee nothing to the company.*" While agreeing with the administrative obstacles, the interviewees were unable to identify the profile best suited to the DPO role, or explain why, or if, their own appointment as DPO complied with the regulations. Nevertheless, the person profile of the DPO was identified as important: *"It must be someone who knows the business very well and is sensitive to the issues.*" (Francis C.) Bernard S., on the other hand, favoured a team model, saying: "*it is safer to have a team with these three valences than a lone DPO."* In conclusion, to overcome this gap, enforcement of a mandatory system is necessary, but due to the DPO being a relatively new role such a system is not currently viable.

4.3 Conclusions: The DPO's influence over strategic decision-making

On the matter of the DPO's influence over strategic decision-making, the respondents defended primarily the role's importance. Michelle P., for example, labelling the role "essential", stated: "*Having*

the DPO is very important, *it is someone highly evaluated, who has the skills necessary to attack the problems and give the necessary guidelines in order to act in a timely way and in the correct manner."* The same interviewee complemented this view with another perspective, that "*The DPO must know the company from the inside. The postholder must know the processes. Oh yes! The DPO can really damage innovation if they don't know the essence of the processes."*

The design of one of the questions in the questionnaire was to attract comment on the statement "*The DPO limits growth and innovation."* The answers, as inferred, were in line with the influence and status that each DPO had within their organization. The interviewees' mainly assumed that the DPO does not limit innovation; on the contrary, the DPO helps to create more efficient and innovative solutions. As Albert C. noted, "*The role of the DPO at this stage is to raise awareness within and of the organization – putting yourself at the heart of innovation and not against it. Otherwise, your position in this role does not fulfil the purpose that was intended. Being on the side of the business, you must also keep up with things. And there must be a mindset around innovation that already incorporates the ideas of innovation."* In contrast, others admitted that the lack of autonomy, tools, or authority to find a solution that met with the interests of both the company and GDPR would inevitably block or limit innovation. Francis C. argued: "*The perception this can give is that the DPO's role limits innovation: increasingly today, if you want to communicate by any means, mainly digital, all that is necessary at the level of resources to comply with the regulation is clearly limiting innovation.*" Two of the other interviewees looked at the issue from an alternative perspective, pointing out that it is the role of the DPO to support decision-making: "*In grey areas, it can clearly support strategic decision-making in order to adapt them to the reality.*" (Michelle P). Meanwhile, Albert C. summed up the question in a simple phrase *"To take no risk is to close the door."*

From the research, the inference is that a consciousness exists that the vision for the role of DPO was not to limit growth and innovation, even though the perception might be that it does so, but accidentally, due to the lack of tools or influence the DPO holds within the organization. Inadvertently, therefore, the DPO may delay or block strategic decision-making. The conclusion to draw from this, in order to overcome this issue, is that were the DPO's role reinforced in the internal corporate governance rule and within the departments and management, the role would earn greater trust and become more efficient.

Following this topic, the interviewees were questioned about the possibility of a veto power. As expected, the answers were in the negative – a veto power does not exist – even while the DPOs did not want to take on such a huge responsibility. Francis C. entertained the hypothesis and stated that a veto *power "Could [step in], but when it is not at all possible to fit the regulations*, *this power appears naturally. [...] The decision not to be able to implement [a veto] should prevail."* Others argued that it would be very useful for the DPO to have the power to veto, in view of the risk relating to the activities of the role. Nonetheless, ultimately, the decision-making power rests with the board. Moreover, if the DPO replaces the board, it is incompatible with the corporate governance principles already in place, as Richard R. pointed out: *"It may be useful, but, ultimately, the decision is made by the executive committee. Personally, I believe more in consent: I think the high school organizations work better, and should I get*

to a point where I had to come to a decision I would not let that happen. I would say that the DPO cannot justify it, if at the same time he is taking personal responsibility." There was a certain consensus that, providing the DPO in post had the skills and influence, the power of veto was not necessary, as "*it never reaches the veto point. The organization has followed the guidelines."* (Albert C.) Alternatively, as Richard R. illustrates: *"In practice you are asked to give your opinion based on the information you hold and the conversations you have had with the company, and then it is up to the board to decide.*" These comments proved to be illuminating insights – suggesting that the veto power may attest to its usefulness, but nonetheless, currently, as the GDPR bestows a great deal of power to the DPO, and this may indirectly block any decision-making powers, it is not in the form of a veto.

Questioned about whether they have intervened in strategic decision-making in the past, either by issuing an unfavourable opinion or, in the extreme, presented a GDPR complaint, the interviewees, fortunately, had never experienced such a situation. The suggestion was that a well-established relationship with the board, along with clear rules of corporate governance allows the DPO, or the board, to exercise their role without the performance of either being limited. In short, one of the interviewees stated that the relationship and its influence on the board consisted of "*the board guiding our proposal for action, or not, by making small adjustments.*" (Albert C.) Nevertheless, the interviewees argued, there is a need for an overall change in mentality regarding the DPO's responsibility and intervention in the organization's decision-making: "*There is a misconception […] people look to the DPO as the person with maximum responsibility, responsible uniquely and exclusively for the protection of data. This poses some difficulties in the DPO's relationship with the company."* (Bernard S.) Ultimately, as a gap already identified, the responsibility falls to the board to make the final decision, while it is the DPO's responsibility to supervise its legality or guide it, even if the implication of this is that the DPO, at some point, could be left with no other option than to present a formal complaint to the regulatory authorities.

As to the future of the DPO's role, some of the respondents, specifically Albert C., defended the evolution of the role: *"In a future model, the DPO will be an external person who provides the organization with their opinions, and articulates these with an area or department of privacy.",* while Michelle P argued that due to the requirements of GDPR, such as the principles of independence and conflict of interest, only an external person could fulfil the purpose envisioned for the DPO's role, as then the postholder *"does not have the restrictions that the regulation imposes on the DPO, like conflict of interest.*", furthermore she also recommended exercising caution, due partly to the DPO's recent introduction. He thought organizations should take great care: *"The DPO may not at this stage be seen by the organization [as important], not in the sense that they can do the job, but in the sense that they must do the job with varying amounts of care.*"

Undeniably, the DPO is more important than imagined by consumers: *"People still do not have a good idea of what the data can generate. Data-owners are not yet aware of the value of the data."* (Michelle P). Due to the value of data, inevitably it will fall to the organization to define the risk, whereby reputational risk will always take precedence over the risk of penalties or fines.

Overall, a gap is evident in the definition of the DPO's role within organizations. This research reveals the various valid arguments and benefits of the different functions each DPO assumes in their respective

organizations. Undoubtedly, there is direct and indirect intervention in the strategic decision-making of organizations, which probably was not part of the initial objective envisioned by introducing GDPR. Nonetheless, while the intervention directives are very much present they are yet undefined. This lack of definition is in itself a gap and is present in many of the gaps identified in this research. Such a lack of definition is not present in similar functions, for example, while the auditor, accountant and compliance function respectively are responsible for auditing, accounting and complying, the DPO's function is less simple to define, as the role acquires many different functions. As all interviewees mentioned in one way or another, the role is still very recent, lacks guidelines, case law or studies to rely upon, and is dependent mostly at present on instinct and community. Many of the actions are, and will be into the near future, based on trial and error, and the consequences of this ad hoc scenario have yet to be fully realized.

To conclude, below the research summary sets out the gaps and inferences in narrative form, while Figure 5 (right) illustrates the same points in graphic form:

1. Recruitment process: companies are entirely responsible for defining the role and appointing a DPO. As there is no uniform or mandated recruitment process, as a consequence the process does not facilitate straightforward external control and permits a large amplitude of the DPO's role;
2. Mentality of the DPO and the role's real function: almost exclusively business-oriented, actively protecting and defending the organization from inherent risks, the DPO's function is inevitably business-oriented to benefit shareholders, and there is an immaterial definition of function for some stakeholders, i.e. the consumer;
3. Value-proposition for the consumer: with a clear business agenda, it was not possible to identify what value the DPO's role actively contributes to the average consumer beyond obligatory compliance with GDPR;
4. External factors: the lack of orientation and the absence of a definition by the supervisory organization, or enforcement/control of the DPO's role presents a risk of non-compliance. Such manifest unawareness is not favourable to allowing the DPO to contribute and influence positively the strategic decisions of the company;

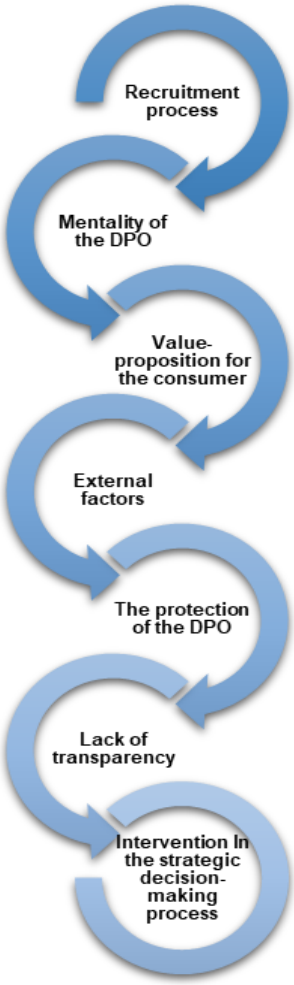

Figure 5: Identified gaps and inferences. Illustration by the

5. Protection of the DPO: currently the measures of protection, over which the DPO has no control, are unrealistic. The inherent consequences of this on the DPO are that it could encourage the postholder not to oppose or influence (unethical) board decisions, which will negatively affect the DPO's influence and relevance both with other stakeholders and the organization;

6. Lack of transparency: makes difficult the function of the DPO and impairs overall trust in the role. Since the role is not easily recognized (externally or internally), this makes limiting and controlling the role easier, but ultimately this limits the development of the DPO's purpose;

7. Intervention in strategic decision-making: it is not clear that it ever was the intention of GDPR to give the DPO's role the level of influence to intervene it currently has. Nonetheless as the reality exists this is the situation to which organizations must adapt. Therefore, it is necessary to regulate its mandate, by limiting or defining its influence within corporate governance.

5 Academic research, practice and final comments

5.1 Relevance of the dissertation for academic research and the business world

A new disruptive reality is shaping the mentality and behaviour of the business world in the twenty-first century. This dissertation has sought to research the impact this is having on organizations at board level and other stakeholders. In addition, the aim of this research has been to delve deeper into this issue — to look at whether the DPO is responsible for exerting influence in the modern technologically driven economy, and also to address the gaps identified during the investigation.

The interest of this dissertation, highlighted in the preliminary research, lies in its appraisal and portrayal of the function of the DPO both in the business world and in academia. This research exercise has resulted in identification of the shortcomings between what the regulation states and its application in practice in the business world. In the researcher's opinion, the dissertation holds interest for professionals involved in the fields of corporate governance, banking as well as risk-management.

The researcher's professional capacity – as the person responsible for the development and implementation of GDPR compliance within corporations – influenced the choice of subject matter chosen for this dissertation. While practising his role, a concern of interest arose as the result of detecting that there was an overall non-definition and uncertainty about the DPO's actual influence and function within organizations. It was notable that the boards of organizations experienced, unexpectedly, difficulty in understanding the nature of the DPO's role, and inevitably this is what has led in large part to the lack of definition and, hence, person specification, when appointing someone to the role. In particular, it has proved intriguing to the researcher to try to understand the future consequences of the appointment, especially since there are no commonly held principles of practice in place.

The current dissertation contributes to academic knowledge by recognizing the relevant gaps. It allows for the identification of potential solutions pertinent to corporate governance principles, such as to "reflect their management's and board of directors' view of the motivations, challenges, solutions and rewards for devising and putting in place better governance rules and practices" (OECD, 2017). The issues relating to the DPO and GDPR are also relevant within the scope of competitive advantage (Porter, 1985) since the research supports the notion that the DPO can affect positively or negatively innovation and development. As such, therefore, the strategy each corporation conveys in its data-use policy and its selection and positioning of its DPO within the organization can result in either a competitive advantage or its opposite.

Admittedly, research into the responsibilities and influence of the DPO within the scope of the role's functions is a relatively under-researched area, in large part because it is such a recent issue, the role only recently elevated by GDPR legislation. Consequently, due to this being an underdeveloped area in both the academic-research and business literature, what at first appears as a problem in need of a solution also offers an interesting opportunity for additional research and investigation. For organizations, their efforts so far to comply with GDPR are only the beginning, for they will be responsible for much of the work undertaken in the future, including the implementation of reviewed and updated codes of conduct, corporate guidelines, as well as the development of an internal control framework and/or stewardship codes.

Finally, this research has sought to understand whether the elevated role bestowed on the DPO after GDPR came into force really affected the paradigm of corporate responsibility. The objective was to conclude whether one consequence of the GDPR's mandate was that it provided the DPO with greater influence over the strategic decision making of organizations. Although the issues raised by this topic at first might not seem important, they have proved to be of great interest. In fact, several indicators suggested during the development of this research that the apparent excessive influence bestowed on the DPO is liable to inhibit the board's decision-making processes.

5.2 Final comments, influencing stakeholders and further research

The data protection laws and the DPO's role in upholding them represent a paradigm shift in corporate responsibility. The DPO's role in its current manifestation has been around for a couple of years to protect both electronic and analogue data in most of the EU member states, while in Germany, for example, these laws have been the reality for the last decade. Thus, German regulation is the basis for most of the rules in relation to GDPR. Nonetheless, the impact is felt most keenly in the principle of privacy by default and the responsibilities imposed, and not simply the mandatory DPO appointment. Organizations know that they must be extra meticulous in their strategic decision-making and in their appointments now that data is no longer a secondary concern but a priority for any organization. Consequently, as the organization's choice of DPO reflects the value the board attributes to this concern, this means that the person (or team selected) should be a highly competent, valued and influential person within the organization. Appointing capable, qualified, aspirational personnel will directly result in the engaged and pro-active performance of the DPO; thus, inevitably, the DPO will directly intervene in the strategic decision-making process or in the definition of the methodology to implement the GDPR strategy in practice, modifying these to suit their own perspective of GDPR compliance.

Without question, GDPR has forced companies to do what they should have been doing all along; that is, to respect privacy and treat data responsibly. The idea that data protection is there to protect the data belonging to individuals, to protect the right to personal privacy, as well as to protect the needs of corporations and governments to collect and benefit from people's personal data, calls for a total change in mentality. This may be the most important aspect of GDPR. Responsible data use and protection of personal privacy were the very things the DPO role was intended to enforce – using all the tools available, including intervening in the decision-making process at board level, even of multi-billion corporations whose direct and indirect impact on society are too relevant to continue to overlook. This

is only achievable with a vertical change in mentality, from top to bottom, within corporations as well as government departments. Undoubtedly, for GDPR to become part of the embedded behavioural culture of organizations requires time. The fact is, however, that in an era when the business world seems motivated only by the idea of profit, only the massive fines and/or threat to corporate reputation the GDPR is allowed to impose for breaches is likely to provide the fuel that will drive the required transformation. Without sanctions such as these, there would be no incentive for businesses to act, and the consumer would be left unprotected. This is particularly concerning, considering the growth of the giant corporations such as Google, Facebook, Microsoft, as well as in the banking and health sector, and yet, importantly, it ought to be stressed that the objective of GDPR is fundamentally not to limit or stop growth and innovation.

Other concerns arise in relation to the subject of the DPO's role that the current dissertation has not directly addressed, but which are nonetheless worth mentioning: these include harmonization and the risk of corporate evasion by moving to favourable (less controlled) jurisdictions within the EU. At the same level, is the idea of a "shop for a compliant DPO"-scenario, which is something that has occurred within the auditing, accountancy and legal market; and then there is the geo-political influence, exemplified by the uncertainty brought about by Brexit.

The future of the DPO in corporate governance will require additional development sector by sector and attention to the definition of the nature of the DPO role itself. New guidelines, case studies, legal precedent, and training will mean that the role is subject to constant evolution, which one day may include certification, implementation of the Fit and Proper regime and updates to the lines of defence and governance models. The effects of the strategies in use now are still to manifest, but nonetheless corporate governance will have to be poised and ready to adapt to the changing paradigm.

Corporation	Listed	Type of DPO Designation	Identification of the DPO	Internal/Outsourced	DPO Need: Based on Complexity Risk	Area
EDP - Energias de Portugal, SA	PSI 20	Privacy Department	Generic Contacts	Internal	Imperative	Energy
REN - SGPS, S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Low	Energy
EDP Renováveis, S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Low	Energy
Galp Energia, SGPS S.A.	PSI 20	Privacy Department	Generic Contacts	Internal	Low	Energy
Société Générale S.A.	CAC 40	DPO Direct Designation	Identifiable physical person	Internal	Imperative	Financial
AXA S.A.	CAC 40	Privacy Department	Generic Contacts	Internal	Imperative	Financial
BNP Paribas S.A.	CAC 40	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Crédit Agricole Group	CAC 40	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Allianz SE	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Deutsche Bank AG	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Bayer AG	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Financial
JPMorgan Chase & Co	Dow Jones	No Clear Designation	No information	No Clear Information	Imperative	Financial
Goldman Sachs Group, Inc.	Dow Jones	Privacy Department	Generic Contacts	Internal	Imperative	Financial
American Express Company	Dow Jones	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Bankia S.A.	IBEX 35	DPO Direct Designation	Identifiable physical person	Internal	Imperative	Financial
CaixaBank SA	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Mapfre, S.A.	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Banco Santander, S.A.	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Banco de Sabadell, S.A	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Banco Bilbao Vizcaya Argentaria S.A	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Bankinter S.A.	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Financial
CTT - Correios de Portugal, S.A.	PSI 20	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Banco Comercial Português S.A.	PSI 20	Privacy Department	Generic Contacts	Internal	Imperative	Financial
Sonae Capital	PSI 20	No Clear Designation	No information	No Clear Information	Medium	Financial
Meliá Hotels International, S.A.	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Hotels
Mota-Engil SGPS, S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Low	Industrial
F. Ramada Aços e Indústrias S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Low	Industrial
Altri, SGPS, S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Low	Industrial
The Navigator Company, S.A.	PSI 20	Privacy Department	Generic Contacts	Internal	Low	Industrial
Corticeira Amorim, SGPS, S.A	PSI 20	Privacy Department	Generic Contacts	Internal	Low	Industrial
Semapa, SGPS	PSI 20	No Clear Designation	No information	No Clear Information	Medium	Industrial
Fresenius Medical Care	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Pharmaceutical
Merck KGaA	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Pharmaceutical
Merck KGaA	Dow Jones	Privacy Department	Generic Contacts	Internal	Imperative	Pharmaceutical
Procter & Gamble Company	Dow Jones	Privacy Department	Generic Contacts	Internal	Imperative	Pharmaceutical
Pfizer, Inc.	Dow Jones	Privacy Department	Generic Contacts	Internal	Imperative	Pharmaceutical
Carrefour S.A.	CAC 40	No Clear Designation	No information	No Clear Information	Imperative	Retail
L'Oréal S.A.	CAC 40	Privacy Department	Generic Contacts	Internal	Medium	Retail
Inditex -Industria de Diseño Textil S.A.	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Retail
Sonae SGPS	PSI 20	No Clear Designation	No information	No Clear Information	Imperative	Retail
Ibersol Restauração, S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Imperative	Retail
Jerónimo Martins SGPS, S.A	PSI 20	Privacy Department	Generic Contacts	Internal	Imperative	Retail
Deutsche Telekom AG	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Technological
SAP SE	DAX 30	Privacy Department	Generic Contacts	Internal	Imperative	Technological
Microsoft Corporation	Dow Jones	No Clear Designation	No information	No Clear Information	Imperative	Technological
Twitter, Inc.	Dow Jones	No Clear Designation	No information	No Clear Information	Imperative	Technological
Cisco Systems, Inc.	Dow Jones	Privacy Department	Generic Contacts	Internal	Imperative	Technological
Telefónica S. A.	IBEX 35	Privacy Department	Generic Contacts	Internal	Imperative	Technological
PHAROL, SGPS S.A.	PSI 20	No Clear Designation	No information	No Clear Information	Imperative	Technological
NOS, SGPS	PSI 20	No Clear Designation	No information	No Clear Information	Imperative	Technological

Figure 2b: Research of DPO in 50 Listed Companies

Figures 3a–3d[1]

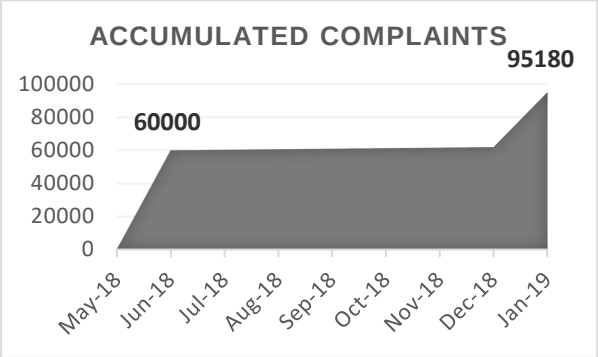

Figure 3a: Accumulated number of complaints to the data protection authorities

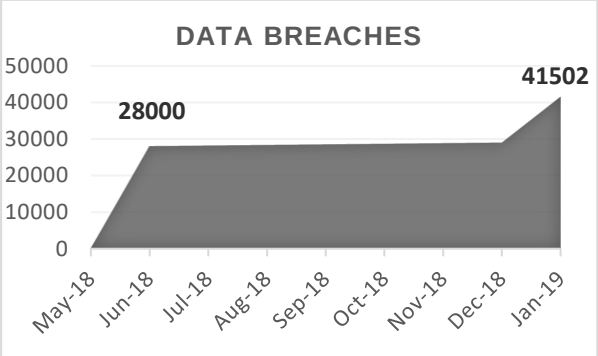

Figure 3b: Accumulated number of data breaches, notifications of accidental or unlawful disclosure by organizations or DPOs

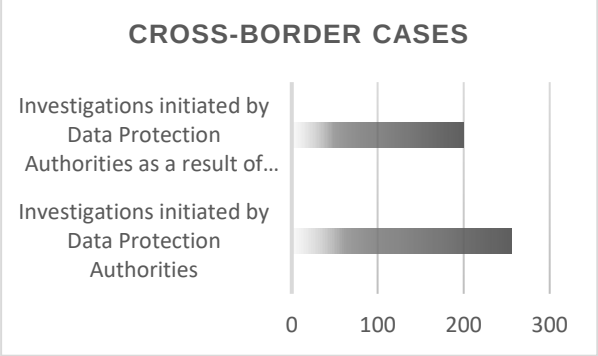

Figure 3c: Cross-border cases between EU member states and third countries

Violation	Value	Location
A social network operator for failing to secure users' data	EUR 20.000,00	Germany
Sports betting café for unlawful video surveillance	EUR 5.280,00	Austria
Google for lack of consent on advertising	EUR 50.000.000,00	France
[2]British Airways security breach and lack of security	£ 183.000.000,00	UK
[3]Marriott Group security breach and lack of security	£ 99.000.000,00	UK
Total number of fines issued in all 28 member states	**3**	
Binding decisions by the European Data Protection Board	**0**	

Figure 3d: Fines issued in all 28 Member States since 25 May 2018 until 11 July 2019

[1] Information for Figures 3a–3c from the European Commission [online] https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf , last accessed 11 July 2019.
[2] Information from the UK Information Commissioner's Office, [online] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ last accessed 11 July 2019.
[3] Information from the UK Information Commissioner's Office, [online] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/ last accessed 11 July 2019.

Figures 4a–4c[4]

Figure 4a: The DPO side by side with senior management, reporting directly to the board.

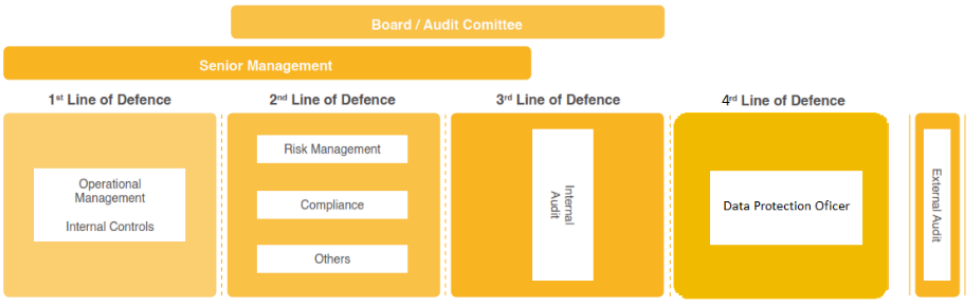

Figure 4b: The DPO role as the fourth line of defence

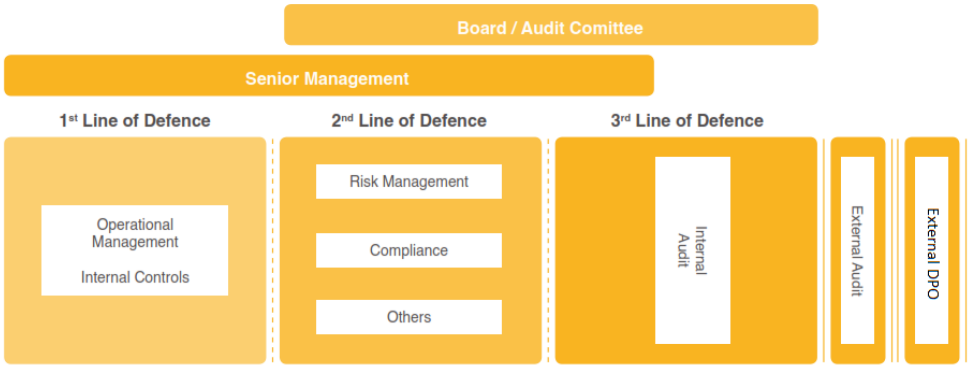

Figure 4c: The DPO acting externally

[4] Figures 4a–4c are the authors own.

References

A&L Goodbody, 2018, *WP29 Guidance on Data Protection Officers (DPOs)*: *A Guide for Businesses* [online] https://www.algoodbody.com/images/uploads/services/WP29_guidance_on_DPOs.pdf (last accessed 18 June 2019).

Agencia Española de Protección de Datos, 2018, *Certification scheme of data Protection officers from The Spanish data protection Agency* [online] https://www.aepd.es/reglamento/cumplimiento/delegado-de-proteccion-de-datos/certificacion-delegado-de-proteccion-de-datos.html (last accessed 18 June 2019).

Article 29 Data Protection Working Party, 2007, *Guidelines on Data Protection Officers ('DPOs')* [online] https://ec.europa.eu/info/law/law-topic/data-protection_en (last accessed 18 June 2019).

Bank of International Settlements, 2014, *Guidelines Corporate Governance Principles for Banks* [online] https://www.bis.org/publ/bcbs176.pdf (last accessed 18 June 2019).

Bank of International Settlements, 2010, *Principles for Enhancing Corporate Governance* [online] https://www.bis.org/publ/bcbs176.htm (last accessed 18 June 2019).

Basel Committee Publications, 2014, *Fit and Proper Principles Paper* [online] http://www.bis.org/publ/bcbs47c4.pdf (last accessed 18 June 2019).

Bellamy, C., 2011, *Elite Interviewing*. DBA Student Conference, 17 May 2011, Nottingham Conference Centre. Nottingham: Nottingham Business School.

Bell, Daniel, 1973, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, New York: Basic Books.

Berufsverband der Datenschutzbeauftragten Deutschlands, 2016, *Code of Practice for Data Protection Officers*, edition no. 3/2016 [online] https://www.bvdnet.de/wp-content (last accessed 18 June 2019).

Bouveret, Antoine, 2018, IMF Working Paper, *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*, International Monetary Fund [online] https://www.imf.org/~/media/Files/Publications/WP/2018/wp18143.ashx (last accessed 18 June 2019).

Bryman, A. and Bell, E., 2007. *Business Research Methods*, 2nd edition, *New York: Oxford University Press*.

CCEPC (Communication from the Commission to the European Parliament and the Council), *Commission guidance on the direct application of the General Data Protection Regulation: Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018* [online] https://ec.europa.eu/commission/sites/beta-political/files/data-protection-communication-com.2018.43.3_en.pdf (last accessed 7 July 2019).

Centre for Information Policy Leadership, 2018, *Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation* [online] https://www.informationpolicycentre.com/cipl-white-papers.html (last accessed 18 June 2019).

Council of the European Union, 1995, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [online] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (last accessed 18 June 2019).

DeFond, M., et al., 2018, "Do Managers Successfully Shop for Compliant Auditors? Evidence from Accounting Estimates", *Law Working Paper No. 432/2018*, European Corporate Governance Institute, [online] http://www.ecgi.global/content/working-papers (last accessed 18 June 2019).

El-Hania, C. N., and Pihlström, S., 2002. *Emergence Theories and Pragmatic Realism* [online] http://www.helsinki.fi/science/commens/papers/emergentism.pdf (last accessed 18 June 2019).

European Banking Authority, 2014, *Guidelines on Internal Governance*, GL 44, https://www.eba.europa.eu/documents/10180/103861/EBA-BS-2011-116-final-EBA-Guidelines-on-Internal-Governance-(2)_1.pdf (last accessed 18 June 2019).

European Banking Authority, 2018, *Opinion of the European Banking Authority on Preparations for the withdrawal of the United Kingdom from the European Union*.

European Banking Authority, 2017, *Guidelines on Internal Governance under Directive 2013/36/EU*, GL/2017/11.

European Central Bank, 2017, *Guide to fit and proper assessments* [online] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.fap_guide_201705.en.pdf (last accessed 18 June 2019).

European Commission, 2019, *Official Infographic* [online] https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf (last accessed 18 June 2019).

European Data Protection Board, 2018, *Information note on data transfers under the GDPR in the event of a no-deal Brexit* [online] https://edpb.europa.eu/our-work-tools/our-documents/drugo/information-note-data-transfers-under-gdpr-event-no-deal-brexit_en (last accessed 18 June 2019).

European Data Protection Board, 2018, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* [online] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under-0_en (last accessed 18 June 2019).

European Data Protection Board, 2018, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [online] https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-22019-processing-personal-data-under-article-61b_en (last accessed 18 June 2019).

European Data Protection Board, 2019, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* [online] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en (last accessed 18 June 2019).

European Data Protection Board, 2019, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)* [online] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en (last accessed 18 June 2019).

European Data Protection Board, 2019, *EU–U.S. Privacy Shield–Second Annual Joint Review* [online] https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en (last accessed 18 June 2019).

European Data Protection Board, 2019, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities* [online] https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-libe-report-implementation-gdpr_en (last accessed 18 June 2019).

European Data Protection Board, 2018, *Statement of the EDPB on the data protection impacts of economic concentration* [online] https://edpb.europa.eu/our-work-tools/our-documents/sonstiges/statement-edpb-data-protection-impacts-economic-concentration_en (last accessed 18 June 2019).

European Data Protection Board, 2018, *Opinion 18/2018 on the draft list of the competent supervisory authority of Portugal regarding the processing operations subject to the requirement of a data-protection impact assessment (Article 35.4 GDPR)* [online] https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-182018-portugal-sas-dpia-list_en (last accessed 18 June 2019).

European Data Protection Board, 2018, *Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan* [online] https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282018-regarding-european-commission-draft_en (last accessed 18 June 2019).

European Parliament and the Council of the European Union, 2016, *Regulation 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, including the preparatory work, studies, papers publish by the European Parliament and the Council* [online] https://eur-lex.europa.eu/ (last accessed 18 June 2019).

European Parliament and the Council of the European Union, 2000, *Charter Of Fundamental Rights Of The European Union*, [online] https://www.europarl.europa.eu/charter/pdf/text_en.pdf, (last accessed 18 June 2019).

European Parliament and the Council of the European Union, 1995, *Directive 95/46/EC, General Data Protection Regulation* [online] https://eur-lex.europa.eu/ (last accessed 18 June 2019).

ENISA (European Union Agency for Network and Information Security), 2018, *Getting Down to Business: ENISA in the EU Cybersecurity Certification Framework* [online] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/getting-down-to-business-enisa-in-the-eu-cybersecurity-certification-framework (last accessed 18 June 2019).

FERMA/ECIIA (Federation of European Risk Management Associations and European Confederation of Institutes of Internal Auditing), *Guidance on the 8th EU Company law Directive, article 41 of the Directive 2006/43/EC* [online] https://eur-lex.europa.eu/ (last accessed 18 June 2019).

Ferraz, D. P., 2012, “Bridging the ‘gap’ between Migrants and the Banking System: An innovative Business Model promoting financial integration, financial stability, and profitability,” DBA Thesis, Cohort 10– 2009/2012. Nottingham: Nottingham Trent University.

Ferraz, D. P., 2011, “Document 4: Structured and Quantitative Research,” 4 January 2011. Supervisors: Professor Alistair Mutch and Professor Colin Fisher, DBA Cohort 10 – 2009/2012. Nottingham: The Nottingham Trent University.

Ferraz, D. P., 2010a, “Document 2: Critical Literature Review, Dual Perspective Field (‘DPF’): A Banking Business Approach to Bridge the Gap Between Banks and Migrants”, Supervisors: Professor Alistair Mutch and Professor Colin Fisher, 8 January 2010. DBA Cohort 10–2009/2012. Nottingham: Nottingham Business School.

Ferraz, D. P., 2010b, *Document 3. Qualitative Research.* Supervisors: Professor Alistair Mutch and Professor Colin Fisher, 1 June 2010. DBA Cohort 10–2009/2012. Nottingham: Nottingham Trent University.

Ferraz, D. P., 2009, “Document 1”, Leading Supervisor: Professor Alistair Mutch, 23 June 2009. DBA Cohort 10– 2009/2012. Nottingham: Nottingham Trent University.

Ferraz, D. P., et al., 2018, “Relationship between top-executive compensation and corporate governance: Evidence from large Italian listed companies”, *International Journal of Disclosure and Governance*, November 2018 [online] https://doi.org/10.1057/s41310-018-0050-2 (last accessed 18 June 2019).

Ferraz, D. P., and D. Castro, Teodora de, 2018, “Fit and Proper: Evitar Um Cisne Negro ou há um Elefante na Sala?”, *InforBanca* no. 114, Nov.2018 [online] http://blog.exed.novasbe.pt/pt/fit-and-proper-evitar-um-cisne-negro-ou-ha-um-elefante-na-sala (last accessed 18 June 2019).

Financial Reporting Council, 2018, The UK Corporate Governance Code, [online] https://www.frc.org.uk/document-library/corporate-governance/2018/uk-corporate-governance-code-2018 (last accessed 18 June 2019).

Fisher, C. M., 2007, *Researching and Writing a Dissertation: A Guidebook for Business Students*, 2nd edition, Harlow: The Financial Times/Prentice Hall.

G20/OECD, 2015, *Principles of Corporate Governance, OECD Report to G20 Finance Ministers and Central Bank Governors*, OECDE [online] https://www.oecd.org/daf/ca (last accessed 18 June 2019).

Goergen, Marc, 2002, *International Corporate Governance*, Prentice Hall.

HEDPL (Handbook on European Data Protection Law), European Union Agency for Fundamental Rights and the Council of Europe together with the Registry of the European Court of Human Rights, 2018, *Handbook on European Data Protection Law* [online] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law (last accessed 18 June 2019).

Hart, C., 1999, *Doing a literature review: Releasing the social science research imagination*, London: SAGE Global Publications.

IAPP (International Association of Privacy Professionals), 2018, *DPO Handbook: Data Protection Officers under the GDPR* [online] https://iapp.org/resources/article/dpo-handbook-data-protection-officers-under-the-gdpr/ (last accessed 18 June 2019).

IAPP (International Association of Privacy Professionals), 2018a*, From Here to DPO: Building a Data Protection Officer* [online] https://iapp.org/resources/article/from-here-to-dpo-building-a-data-protection-officer/ (last accessed 18 June 2019).

IAPP (International Association of Privacy Professionals), 2018b, *The Mandatory DPO* [online] https://iapp.org/train/gdprready/ (last accessed 18 June 2019).

Ireland, 2018, *Data Protection Act of 2018* [online] http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html (last accessed 18 June 2019).

IPCG (Instituto Português de Corporate Governance), 2018, *Código de Governo das Sociedades do IPCG* [online] https://cgov.pt/regulamentacao/codigos-de-governo/1235-codigo-de-governo-das-sociedades-2018-encontro-de-apresentacao (last accessed 18 June 2019).

International Association of Insurance Supervisors, 2000, *Guidance Paper For Fit and Proper Principles and their Application* [online] https://www.iaisweb.org/index.cfm?event=getPage&nodeId=25283 (last accessed 18 June 2019).

Lambert, Paul, 2016, *The Data Protection Officer: Profession, Rules, and Role*, Association of American Publishers: Auerbach Publications.

Lenoble, J., 2003, *An Institutionalist Approach*, Kluwer Law International.

Leplin, J., 1984, *Scientific Realism*, Berkeley, CA: University of California.

Miles, M. B., and Huberman, A. M., 1994, *An Expanded Sourcebook: Qualitative Data Analysis*, 2nd edition, London: Sage.

Mounce, H. O., 1997, *The Two Pragmatisms: From Peirce to Rorty*, London: Routledge.

OECD, 2019, *The OECD Ministerial "Declaration on the Protection of Privacy on Global Networks",* OECD Legal Instruments [online] https://legalinstruments.oecd.org/public/doc/109/109.en.pdf (last accessed 18 June 2019).

OECD-PF, 2013, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OCDE* [online] https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (last accessed 18 June 2019).

Porter, M. E., 2001, *Strategy and the Internet*, Harvard Business Review.

Porter, M. E., 1996, *What is Strategy?,* Harvard Business Review.

Porter, M. E., 1985, *Competitive Advantage, New York,* Free Press.

Porter, M. E., 1980, *Competitive Strategy*, New York: Free Press.

Rescher, M., 2000, *Realistic Pragmatism: An Introduction to Pragmatic Philosophy*, Albany, NY: State University of New York.

Regierungskommission Deutscher Corporate Governance Kodex, 2017, German Corporate Governance Code, [online] https://www.dcgk.de/en/code.html (last accessed 18 June 2019)

The Committee on the Financial Aspects of Corporate Governance, 1991, Cadbury Report - Financial Aspects of Corporate Governance [online] https://ecgi.global/download/file/fid/9448 (last accessed 18 June 2019).

UK Information Commissioner's Office, 2019, [online] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/ last accessed 11 July 2019.

UK Information Commissioner's Office, 2019, [online] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-ico-announces-intention-to-fine-british-airways/ last accessed 11 July 2019.