International Journal of Economics and Business Administration
Volume VII, Issue 4, 2019

pp. 243-266

The Impact of the General Data Protection Regulation on the Financial Services' Industry of Small European States*

Submitted 15/08/19, 1st revision 22/09/19, 2nd revision 21/10/19, Accepted 10/11/19

Kieran Xuereb[1], Simon Grima[2], Frank Bezzina [3], Andre Farrugia [4], Pierpaolo Marano[5]

Abstract:

Purpose: *With this paper we evaluate the impact and implications of the European Union (EU) General Data Protection Regulation (GDPR) on the Financial Services Industry in small European States; specifically Malta, Slovenia, Luxembourg, Lithuania, Latvia, Estonia and Cyprus. That is, countries within the EU having less than 3 million population.*
Design/methodology/approach: *We collected our primary data by carrying out scheduled semi-structured interviews (using WhatsApp®, Messenger® and Skype®) with 63 participants who are working directly or indirectly with GDPR in financial services between November 2018 and April 2019. The interview was structured using two impact themes, 'Trust, Standardisation and Reputation' and 'Training and 'Resources', with 18 statements under each theme to which participants were required to answer using a 5-point Likert-scale ranging from "Strongly Disagree" to "Strongly Agree". To answer the research questions, the empirical data collected was subjected to statistical analysis using SPSS (Version 21) namely descriptive statistics and box plots and later MANOVA, while the qualitative data was analysed using the thematic approach.*

[1]*Graduate Banking and Finance, Department of Banking and Finance, Faculty of Economics, Management and Accountancy,University of Malta, Kierankxuereb@gmail.com*
[2]*University of Malta, Department of Insurance, Faculty of Economics, Management and Accountancy, corresponding author, simon.grima@um.edu.mt*
[3]*Dean, University of Malta, Department of Management, Faculty of Economics, Management and Accountancy, Email: Frank.Bezzina@um.edu.mt*
[4]*University of Malta, Department of Insurance, Faculty of Economics, Management and Accountancy, Email: andre.farrugia@um.edu.mt*
[5]*Associate Professor, Department of Insurance, Faculty of Banking, Financial and Insurance Science, Catholic University of the Sacred Heart - Milan Pierpaolo.Marano@unicatt.it*

**This paper is based on the unpublished Thesis by Magri, A. (2018). An Evaluation of the Impact of GDPR on the Local Financial Services Industry. Banking and Finance, Department of Banking and Finance, Faculty of Economics, Management and Accountancy, University of Malta, supervised by Dr. Simon Grima.*

Findings: *We found that overall, participants feel that although GDPR has increased the work load and costs, it has helped to improve the trust, standardisation and reputation of the institutions they represent. However, this comes with some repercussions from the data subjects who are not conversant with the regulation and are apprehensive by the consents required.*

Originality/value: *Although, all States might be represented in the decision process, the larger States usually take over and sometimes dictate the final decision. The concept of proportionality in regulations is not clean and is not effectively managed, at the disadvantage of the smaller States. Therefore, this paper is important since it voices the cries of smaller States and allows for an understanding of the impact and implications of new regulations to smaller jurisdictions, in this case within the EU.*

Keywords: *GDPR, regulations, small EU states, financial services industry, reputation.*

JEL Codes: *G1, G2, G32, G15,G26,G41, K12, L5, D53, E44.*

Paper type*: Research Article*

1. Introduction

The General Data Protection Regulation (GDPR) comprises of a new set of regulations that govern data protection in Europe. Organisations, which collect and process data, must adhere to the detailed and numerous requirements within the regulation. One of the main industries that has been affected by this regulation is the Financial Services Industry. The requirements of the GDPR may be identified under various themes, namely the Data Subject's Consent, Right of Erasure, Right to Portability, Right to not be subject to Profiling, Data Breach Incident Response Plan, Breaches and their Consequences, appointment of the Data Protection Officer (DPO), Data Encryption, Privacy by Design and Vendor Management. These requirements have both positive and negative impacts on a financial services organisation. These impacts can relate to various aspects such as 1) the level of trust towards the organisation and reputation of the financial services firm, 2) training needs and 3) internal policies, procedures and resources requirements.

The objective of this paper is to lay out the analysis of the perceived impact and implications of complying with the European Union (EU) GDPR on the Financial Services Industry in small European States; specifically Malta, Slovenia, Luxembourg, Lithuania, Latvia, Estonia and Cyprus. That is, countries within the EU having less than 3 million population. Specifically, we would like to determine the perceived impact and implications of GDPR on 1) the level of trust towards the financial services firm and the respective reputation, 2) the training needs, 3) the internal policies, procedures and resources requirements. In doing this, we would like to understand whether these levels vary as a function of the type of firm (administrative vs customer-oriented).

GDPR came into force on the 25th of May 2018, affecting all organisations that operate in the European Union (EU) and collect and process personal. However, as far as we understand no study has yet been carried out on the impact and implications that this requirement will have on the financial services industry in EU small jurisdictions. Therefore, this study is important for policy makers and persons involved in building strategies within the financial services industry since it will shed light on the grey areas that this legislation brings with it. This study adds value to the findings of various prominent researchers such as King (1993), Briguglio, (1995), Baldacchino (2006), Bezzina *et. al.* (2012; 2014) who highlight the importance of the use of small states as small scale laboratories for more complex politics, regulations and policies of larger countries.

Although, all States might be represented in the decision process, the larger States usually take over and sometimes dictate the final decision. The concept of proportionality in regulations is not clean and is not effectively managed, at the disadvantage of the smaller States. A proportionate approach would mean tailoring regulatory requirements to 1) firm's size, 2) systemic importance, 3) complexity and risk profile, to avoid excessive compliance costs and regulatory burden for smaller and non-complex organisations that could unduly reduce their competitiveness without justification (Lautenschläger, 2017). Most regulations within the EU are drawn-up by representatives of larger States and a one-size-fits-all approach is taken.

Therefore, this article is important since it voices the cries of smaller States and allows for an understanding of the impact and implications of new regulations to smaller jurisdictions, in this case within the EU.

2. Literature Review

Processing and controlling of personal data, has always been crucial for institutions as this helps coordinate the data and findings retrieved from different sources (Unisoftatatech Blog, 2016). As a result of major developments in technology, the processing and controlling of data has become a prerequisite (Rossow, 2018). Once collected and sorted, data should be easy to understand. Data protection has been regulated for many years with the first European Data Protection Directive (Directive 95/46/EC), coming into force in October 24th, 1995. Since an EU Directive is a requirement every European Member State had to follow or implement the European Data Protection Directive and transpose it into its own, regulatory framework. This directive standardised the way to protect individuals with regards to personal data processes and the free movement of data (European Data Protection Supervisor, n.d.). As Nate Lord (2018) highlights, the Directive was built on seven main principles:

- Purpose – There needs to be a purpose as to why a person's data is collected.
- Notice – The individual is informed when his/her personal data is

collected.

- Consent – Consent is given by the individual before his/her information is shared.
- Security – Personal data is secured.
- Disclosure – Much like *Notice*, data collectors need to disclose when an individual's personal data is being collected.
- Access – The individual's ability to access his/her data and have the right to amend any information.
- Accountability – Data collectors are responsible for properly following the previous six steps.

As per the Data Protection Directive, any information that can be linked to an individual, fits the definition of personal data. This means any information that relates to an identifiable person; being either by the names, physical identity, mental identity, Identification Number, Credit Card Numbers, home or work addresses (European Parliament and Council, 1995).

The benefit of this directive was that it brought to light the importance of personal data protection. This Directive regulates parties that operate within or outside any EU Member State, making use of personal data of individuals situated in any EU Member State. Data controllers had the obligation to notify the governing body before they could make use of personal data. Such obligation had to include several specifications, including the intended use, the name and address of the controller, what type of data needs to be collected and what type of protection measures are being taken to ensure that data is secure both in the short and long term (Lord, 2018). Throughout the years, there were some additions to the Directive to cater for technological advancements in the way people communicate. An important addition was the emergence of the Internet. Back in the 1990's and the early 2000's, only a small number of European citizens had access to the Internet, thus, online privacy concerns were negligible (Tjalsma, 2017).

The use of the Internet has increased at such a rate that online privacy concerns became more prominent. This has caused changes in the way we collect, store, use and transfer personal data. Eventually the EU Data Protection Directive became insufficient, and therefore, the EU had to come up with a new regulation (Rossow, 2018).

2.1 The Need for the GDPR

With a new and improved regulation, the EU Commission hoped that it would be more up-to-date with current times and that every member state would have to abide by the same set of rules. Late in 2015, the European Parliament, the European Council and the European Commission came to an agreement on the new data protection rules, which were grouped to form the GDPR, which supersedes the older directive. The GDPR is a collaborative exercise across all the EU Member States and

which was approved by the European Parliament on the GDPR on the 14th of April 2016 (Lord, 2018). On the 2nd of February 2016, the EU and the United States (US) came into an agreement regarding exchanging personal data for commercial purposes between the EU Member States and the US. The main aim for such an agreement was to facilitate exchange and to protect the individual's personal data (The International Trade Administration, n.d.).

The GDPR establishes a new and improved set of rules on every organisation. These include the Government and different types of companies, that offer services to people who are situated in EU countries and even for data that may not be worked on in EU countries but relates to EU residents. The new regulation is simpler, and according to Evelyn Wolf (2018), it hopes to regain citizens' trust which may have been lost due to the financial institution scandals or due to enforced marketing techniques. Each member of the EU must apply and enforce this regulation (Tjalsma, 2017). The GDPR builds on principles of the old directive and gives additional focus to specific data protection requirements with robust enforcement and larger penalties if companies do not comply with the regulation. Also, individuals are given more control over their own personal information (Lord, 2018).

Even though data protection laws have become stricter, once an organisation manages to fully embrace these rules, it will be able to participate in any business that occurs across the EU. However, organisations that do not comply with the key provisions of GDPR can face penalties up to € 20 million or 4% of the organisations' annual revenue. If non-compliance is related to technical measures, such as, breach notifications and impact assessments, institutions can be fined an amount greater than €10 million or 2% global annual revenue from the previous year (GDPR Report, 2017).

2.2 Themes of the GDPR

These are the different requirements that emerge from the regulation, which organisations must abide by to ensure that they are compliant. Financial Services Institutions already face stringent regulations and oversight requirements, and under the GDPR, this has increased. Organisations rely on obtaining data to enhance their decision making, to detect fraud, for compliance requirements and risk management (Siegler, 2018).

2.2.1 Theme 1: Data Subjects' Consent

Personal data under the terms of GDPR refers to anything that that can be used to identify an individual such as by name, email address, IP address, profiles on social media or social security or identification numbers (Brickendon Consulting Limited, 2018). Organisations in the Financial Services Industry are responsible for acquiring consent before collecting and processing such data and must also maintain a record of when and how the customers were made aware of it. Moreover, individuals also

have the right to withdraw their consent and regular consent reviews should be carried out to ensure compliance with the regulation.

According to Frederik Van Remoortel (2016), consent needs to meet certain criteria. This entails that is must be freely given by the data subjects and specific for particular services. Unambiguous consent forms shall be presented to data subjects to inform them as to why and how their data is being requested and processed. Institutions; being directly or indirectly involved in the financial services industry, should evaluate the legitimate basis of their processing operations. In some cases, consent that has been previously given, would no longer be suitable under GDPR and would have to be obtained again. There is also the possibility that data is transferred between different organisations, such as transfer between the data processors and controllers. Such a possibility can be feasible if the data subjects have given prior consent and it is technically feasible (Rossow, 2018).

Data can also be transferred to a third country. Such transfer can only be possible if there are acceptable levels of protection in a particular country and if the data subject concerned, has given his/her explicit consent (Office of the Information and Data Protection Commissioner, 2018).

2.2.2 Theme 2: Right to Erasure

The right to data erasure or the right to be forgotten, gives individuals the right to request organisations to erase any personal data that belongs to them, unless this data is no longer needed, such as for example to comply with other regulations such as AML Regulations and for legal purposes. This also applies to data that the organisation shares with third-parties. In order to execute such requests, organisations need to have efficient and robust data inventories (Brickendon Consulting Limited, 2018).

Another right that ties in with this right is *'Right to Rectification'*. If the data stored is incorrect, the data subject has the right to request data controllers to amend the data and data controllers have the duty to notify the other parties involved (Office of the Information and Data Protection Commissioner, 2018).

2.2.3 Theme 3: Right to Portability

Data Subjects have the right to request which data the organisation is processing about them and to receive the response in a structure, commonly-used and machine-readable format (GDPR- Info, n.d.). According to Luke Irwin (2018), the data that the data controller must provide to the data subject, should include data provided by the data subject and the observed data by the controller such as search history and location data.

2.2.4 Theme 4: Right not to be subject to Profiling

Article 22 of the GDPR stipulates that individuals have the right not to be subjected to profiling or to automated decision-making unless explicit consent is given,

necessary for the business relationship or authorised by law. With regards to credit institutions, this can apply to Credit Scoring[6]. Data subjects can request for a decision to be re-evaluated if that decision was based on automated processing (Office of the Information and Data Protection Commissioner, 2018).

2.2.5 Theme 5: Breaches and their Consequences

With regards to personal data breaches, GDPR has rigorous requirements. A personal data breach refers to any breach of security leading to the destruction, loss or modification of personal data. Any organisation has 72 hours to inform the relevant supervisory authority about such breach once they have been made aware of it. Such notification should include details regarding the nature of the breach, the individuals impacted and contact information of the DPO (Brickendon Consulting Limited, 2018). If the breach is deemed as high risk, then the data subject should also be notified. Organisations should keep record of such breaches (Office of the Information and Data Protection Commissioner, 2018).

2.2.6 Theme 6: Right to Erasure

The right to data erasure or the right to be forgotten, gives individuals the right to request organisations to erase any personal data that belongs to them, if this data is no longer needed, such as to comply with other regulations such as the Anti Money Laudering (AML) Regulations and for legal purposes. This also applies to data that the organisation shares with third-parties. In order to execute such requests, organisations need to have efficient and robust data inventories (Brickendon Consulting Limited, 2018). Another right that ties in with this right is 'Right to Rectification'. If the data stored is incorrect, the data subject has the right to request data controllers to amend the data and data controllers have the duty to notify the other parties involved (Office of the Information and Data Protection Commissioner, 2018).

2.2.7 Theme 7: Data Breach Incident Response Plan

Financial Services organisations should ensure that they are well prepared for anything that can happen with regards to the GDPR. Andrew Rossow (2018), cited that organisations should have a Data Breach Incident Response Plan. For most organisations, this is not something new as they already have this response plan in place. However, this needs to be suited to the requirements of the GDPR. Organisations must test these plans beforehand to make sure they are functioning properly. The quicker the data response team can familiarise themselves with the plan, the better for breach reporting and thus, the lesser the potential penalties.

2.2.8 Theme 8: Data Protection Officer

According to Nate Lord (2019), the European Parliament, European Council and the European Commission make the role of the DPO mandatory for those organisations

[6]*Credit Scoring measures the possibility of default from debt obligations by an individual or corporation.*

that store and/or process a considerable amount of personal data. Andrew Rossow (2018), adds that the person appointed as the DPO can already hold a similar role in the organisation, as long as there would not be any conflict of interest and is able to provide protection of the personally identifiable information (PII)[7].

A DPO has the responsibility to supervise the data protection strategy and to make sure that GDPR requirements are being implemented correctly and adequately. Nate Lord (2019), mentioned that a DPO has to be appointed for all public organisations and where the core activities of the controller/processor involves regular monitoring of data subjects and where the organisation conducts considerable processing of 'special categories' of personal data[8]. The DPO must be very knowledgeable about what GDPR states and how this can affect the organisation. A DPO is responsible for educating the company and its employees with regards to being compliant with the regulation, giving training related to the processing of data to staff and conducting frequent security checks. A DPO also acts as the point of contact between the organisation and the supervisory authority. Other responsibilities include monitoring the performance of the company and giving advice regarding data protection efforts, maintaining record of all data processing activities and the purpose of such processing and providing information to data subjects on how their data is being used, on their rights and what the organisation is doing to make sure that the data is secure (Lord, 2019).

The DPO's expertise needs to be aligned with the data protection operations and the level of data protection required by the organisation. For an organisation to hire a DPO, it must make sure that the individual understands completely the organisation's IT infrastructure. A DPO should have exceptional management skills and good communication skills to have a good rapport inside and outside the company (Lord, 2019).

2.2.9 Theme 9: Encryption and Pseudonymisation of Data

It is important that all data is encrypted and in a pseudonymised form. Pseudonymisation is a security technique that is required under GDPR. If a financial services organisation fails to anonymise data, the organisation would be faced with a data breach and its consequences (Deloitte Malta, n.d.). For a company to comply with GDPR, data should be pseudonymised into artificial identifiers thus ensuring that the data remains on a 'need-to-know' basis (Brickendon Consulting Limited, 2018).

2.2.10 Theme 10: Record of the risks involved

Andrew Rossow (2018), wrote that institutions should create a record or log of risks and compliance progress within the institution. This is known as the Data Protection Impact Assessment. This record should include the progress that the organisation has

[7]*Any data that can identify and distinguish individuals.*

[8]*Data that refers to race, ethnicity and religious beliefs of the data subjects.*

made with regards to GDPR, showing which risks they are susceptible to and how they will try to minimise or eliminate them**.**

2.2.11 Theme 11: Privacy by Design

Following a breach, supervisors are required to examine what measures has the organisation followed in order to protect personal data. This is done in order to determine fines. Privacy by Design refers to all accountability for compliance and data protection measures taken by organisations. It requires organisations to show their organisational and technical controls and how these relate to compliance; not just in reports but also how the company is run (Siegler, 2018).

2.2.12 Theme 12: Vendor Management

At the core of every financial institution, there is data which is being shared through different IT applications. It is very important that financial services institutions have clear procedures in place with vendor companies[9] that are handling data. Most organisations would require the expertise of such vendors to process data. Therefore, procedures need to be in place and agreed upon between the parties to ensure that there are no breaches (Siegler, 20).

2.3 The Impacts of the GDPR

The themes extracted from the GDPR, have and will, in some way, leave or have already left an impact on the Financial Services Industry.

2.3.1 Positive Impacts

2.3.1.1 Trust and Reputation

Being more GDPR compliant can support the organisation in building a more trusting relationship with the customers and the general public. Customers are becoming more aware and suspicious about the way their personal data is being used, thus by being transparent, the organisation will become more trustworthy (Fimin, 2018). The proper use of cookies on the organisation's website can also display trust. Customers should be informed that cookies are being used and for what reason. It should be possible for customers to opt-in as well as opt-out of the various cookies (Cookiebot, n.d.).

Although the potential fines are quite significant, reputation is something that cannot be overlooked. Reputation should be one of the main concerns for organisations, regardless of the industry. Failure to meet the requirements of GDPR can become a very public affair (Wright, 2018).

[9]*Vendor companies offer a product or service to other companies such as banks, in the form of IT software and programs that aid banks in their duties such as with data processing.*

For an organisation to safeguard its reputation, it is vital to be prepared for anything that can happen. The organisation needs to be ready for the first data breach or a request from data subjects. Data subjects will less likely request to view their personal data if they trust the organisation. Responding quickly to data subjects, in a transparent manner will generally reduce the risk of attacks to the organisation's privacy policy (Mommers, 2018).

2.3.1.2 Training provided to Employees

In order for the organisation to be GDPR complaint, privacy training given to the employees is vital. It is useless for an organisation to fulfil all the other steps of GDPR compliance without training its employees on how they should handle personal data and how to be attentive so that the organisation does not suffer from cyber-attacks (Kotur, 2018). The organisation and the DPO have the duty to raise awareness about data protection and provide adequate and continuous training to the employees involved in the process of collecting and maintaining personal data. With the number of data protection breaches increasing, its important to train the employees so that they know how to protect personal data (Kotur, 2018).

2.3.1.3 Cybersecurity Improvements

One of the main reasons why the EU deemed that it needs to introduce new data protection regulations was because of the increased use of the Internet and the new ways of how organisations gather and process personal data. Before the GDPR, organisations faced an endless battle with cybersecurity.

Until recently, the primary sources of cyber security have been security upgrades in servers and infrastructures. With the implementation of GDPR, data privacy and security standards have been directly impacted whilst also the regulation encourages organisations to limit the risks of data breaches and improve their cybersecurity measures (McGavisk, n.d.). Any organisation cannot afford to ignore cybersecurity measures as the costs of data breaches, loss of business and trust, are substantial. GDPR encourages organisations to re-evaluate their overall cybersecurity strategy by establishing a thorough control of the entire IT infrastructure and building robust data protection workflows (Fimin, 2018).

2.3.1.4 Standardisation of Regulation

Organisations are assessed by the national Data Protection Agency. Although these assessments carried out by the national agencies, since the GDPR is a standardised EU regulation, once an organisation is deemed as compliant, it is free to operate throughout all European countries without being required to deal with each national data protection legislation (McGavisk, n.d.).

2.3.1.5 Better use of Human Resources

Organisations have a vast amount of sensitive and confidential data that they must process. Before the GDPR, certain information might have fallen in the wrong hands since certain employees might not have known the value of said data. With the

GDPR, certain data access is given to a few professionals, since the handling data comes with greater levels of responsibility (Hadabas, 2018).

2.3.1.6 Efficient use of IT Resources

Data controllers and processors share compliance requirements and together they need to ensure that the processing of data is performed in compliance with the regulation. Organisations assess which IT systems help them meet demands more efficiently. New systems that ensure the organisation will remain secure from any breaches or failures, would be investigated (Baker & Lampaki, 2017). As the data that organisations hold is more streamlined, the IT systems may be more efficiently used. According to Trevor Hughes, the president of the International Association of Privacy Professionals, organisations are cleaning up any unnecessary data that is spread across the organisation (Khan, 2017).

2.3.1.7 Efficient use of Time

Before the GDPR, organisations held a lot of data which ultimately resulted in data chaos. Certain data was kept by organisations even if there was no use for it. After the introduction of GDPR, efficient time management and consumption became important and organization did not want to waste time and efforts on things that do not concern them (Baker & Lampaki, 2017).

2.3.2 Negative Impacts

2.3.2.1 Extensive Training

Although it is important for organisations to provide training to employees, this could lead to extensive training that rather than benefits the organisation, it could negatively impact the organisation. For an organisation to have a culture of data protection across all its business areas, training on a large scale can be depressing for those involved. Employees will not take training seriously and positively. Certain training can also be irrelevant and not pertaining to the employees' own activities (Kotur, 2018).

2.3.2.2 Increase pressure on Human Resources

Apart from the positive impacts on human resources, GDPR has also negatively affected human resources. With GDPR, there are greater pressures on human resources to safeguard sensitive data and ensure that no confidential information is accidentally exposed. Organisations need to take measures to ensure that identifiable information is minimised, and that unnecessary data is removed. The regulation also requires all data processing to have a lawful basis and, in some scenarios, explicit consent is required. This requires employees to ask for specific and unambiguous consent from the data subject which may put more pressure on human resources (Hadabas, 2018). As it is required that personal data should be updated, employees are under pressure to ensure that personal data is accurate so that there would not be any breaches. In case of a breach, employees are put under pressure since they must report the breach to the supervisory authority within 72 hours and explain the reason

behind the breach (Hadabas, 2018). Organisations must also develop data protection processes that will be shared throughout the entire organisation. Data Protection by Design ensures that knowledgeable employees are given the task to process personal data (Hadabas, 2018).

2.3.2.3 Increase in the use of IT Resources

For data controllers and processors to ensure security when controlling and processing data, the appropriate technical measures, being IT software and applications used, must be implemented. Such measures are important to ensure appropriate levels of security to cover for the risks, which include the encryption and pseudonymisation of data (Baker & Lampaki, 2017). GDPR compliance will demand sufficient technical investment from organisations. Organisations will have to invest in software to ensure that they are compliant with the regulation (Lilkov, 2018).

2.3.2.4 More burden on Financial Resources

The cost of compliance with the GDPR is substantial. From a survey conducted by PwC, it was highlighted that 68% of the organisations were willing to spend in the region of $1 million to $10 million to ensure compliance. Meeting the privacy requirements of the GDPR is not an easy and cheap task (Baker & Lampaki, 2017). On the other hand, failure of the organisation to comply with requirements of GDPR may be more costly and have a domino effect on the other resources. One of these is the organisation's financial resources. Organisations that fail to comply, risk being penalised and having to pay huge fines that may be up to €20 million. Such money could be used more efficiently elsewhere such as for improving training, IT resources and employment of knowledgeable personnel (Baker & Lampaki, 2017). Those organisations that employ more than 250 employees, are public and regulatory monitor individuals on a large scale or process special categories of data are required to hire a DPO. Such appointment can be costly and increases the financial burden on the organisation (Baker & Lampaki, 2017).

2.3.2.5 Increase in Time-Consumption

As organisations fear that the workload will increase, more time will be allocated to ensure that data privacy processes are working as they should. Although an organisation may feel that maintaining a lot of consumer and employee data is beneficial, such practice is very time-consuming. Organisations need to apply the 'less is more' rule where it is beneficial to use less time and effort on something that is not of any value and in turn use time and effort for something that offers value (Baker & Lampaki, 2017).

3. Methodology

3.1 The Research Instrument and Sample Procedure

To carry out this study and reach our objectives we carried out 63 semi-structured scheduled interviews (using telephone and skype) with whom we deemed as or where directed to, experts in the field of Data Protection, mainly Data Protection Officers (DPO)s and compliance officers (i.e. purposive and snowballing sampling) (Naderifar *et al.,* 2017). We stopped carrying out interviews when a saturation point was achieved and no further value was gained from an extra interview (Saunders *et al.,* 2018). The interviews consisted of 1 demographic question (Q36) which related to the nature of the business (Administrative or Customer-Oriented), '35' statements under 4 themes (i.e. *1. Trust towards the financial services firm and their respective reputation* (Q1 to Q9), *2. Training Needs* (Q10 to Q15), and *3. Internal Policies, Procedures and Resource requirements* (Q16 to Q35)) to which the participant needed to answer according to a 5-point Likert scale ranging from 1 - 'Strongly Disagree' to 5 - 'Strongly Agree' and a final question to which participants were free to open up and provide an opinion or comment further (Q37).

All interviews were carried out, by the authors and with the help of peers from the different countries, between November 2018 and August 2019, either face-to-face or using the phone and Skype. To answer the research questions, the empirical data collected was subjected to statistical analysis using SPSS (Version 21) namely descriptive statistics and box plots and later MANOVA, while the qualitative data was analysed using the thematic approach.

3.1.1 Research Questions

RQ1: In the light of the impact and implications of GDPR, what are the levels of (i) trust towards the financial services firms and their respective reputation, (ii) training needs, and (iii) the internal policies, procedures and resource requirements?

RQ2: Do these levels vary as a function of the type of firm (administrative vs customer-oriented)?

3.1.2 Data Analysis Procedures

The open-ended answers were later transcribed onto one Ms word document and anlaysed using the thematic approach (Braun & Clarke, 2006), while the closed-ended answers were put into excel and later into SPSS to enable further analysis.

To answer **RQ1,** descriptive statistics and box plots were generated for each of the three variables – *i) trust and reputation, ii) training needs and iii) internal policies, procedures and resources requirements* (hereafter, resources) – to obtain information on measures of central tendency (mean and median) and spread (range and inter-quartile range), and to illustrate the data graphically.

To answer **RQ2,** multivariate analysis of variance (MANOVA) was used, with three dependent variables – (i) level of trust, (ii) training needs, and (iii) resources – and

business type (1 = administrative firms comprising fund administrators (7.9%), audit firms (12.7%) and company services providers (28.6%), and 2 = customer-oriented firms comprising credit institutions (15.9%), financial institutions (15.9%) and insurance firms (19%)) as an independent variable (or fixed factor).

In preliminary analysis, descriptive statistics were generated and group means and standard deviations for each dependent variables. The Levene's test was also generated to ensure that the error variance of each dependent variables was equal across groups while the Box's Test was used to ensure that the population variance-covariance matrices of the different groups in the analysis were homogeneous (Field, 2009). Then, the MANOVA test-statistics were generated to determine the dependent variables varied as a function of business type.

3.1.3 Limitations

When conducting interviews, the interviewer was aware of the probability that most interviewees would be pre-prepared to answer certain questions. Such responses can be subjective and might change over time (Alshenqeeti, 2014). In addition to this, interviews are time-consuming with regards to both collection and analysis of data. The author had a limited time frame to collect and analyse the interviews. This may hinder the number of responses gathered and the possibility to ask more in-depth questions that may be relevant for this study (Alshenqeeti, 2014).

Moreover, using a 5-point Likert Scale only gives the respondent unidimensional and limited choices to choose from. The distance between the options; ranging from "Strongly Disagree" to "Strongly Agree", cannot be equidistant (Sullivan & Artino, Jr, 2013). Also, the respondents may avoid using the "extreme" options on the scale even if such choices would be the most accurate (Bishop & Herron, 2015).

4. Results

*Theme 1 - Trust and Reputat*ion (Q1 to Q9): The statements in section 2 theme 1, was aimed at determining whether participants perceived that the level of trust towards institutions, more precisely Financial Institutions has increased. Following the implementation of GDPR. The Cronbach alpha revealed that the measures of the grouped themes (Q1 to Q9) were internally consistent with scale reliability (Cronbach's $\alpha = 0.89$, n=9).

Theme 2 - Training Needs (Q10 to Q15): The statements in section 2 theme 2, was aimed at determining whether participants perceived that in order for employees to have a better understanding of the requirements of GDPR and its impacts on the organisation, the organisation needs to organise and provide training with regards to data protection to its employees. Moreover, we also wanted to determine whether participants feel that the GDPR has affected internal policies and procedures of their organisation. The Cronbach alpha (Q10 to Q15) revealed that the measures of the

grouped themes were internally consistent with scale reliability (Cronbach's α = 0.91, n=5).

Theme 3 - Internal Policies, Procedures and Resources (Q16 to Q35) : The statements in section 2 theme 3, was aimed at determining whether participants perceived that for an organisation to be compliant with GDPR and its requirements, the use of the organisation's resources will be impacted (i.e. Financial, human, time, IT and software resources). The Cronbach alpha revealed that the measures of the grouped themes were internally consistent with scale reliability (Cronbach's α = 0.79, n=20). Table 1 provides the descriptive statistics table for three variables - trust and reputation, training needs and resource requirements.

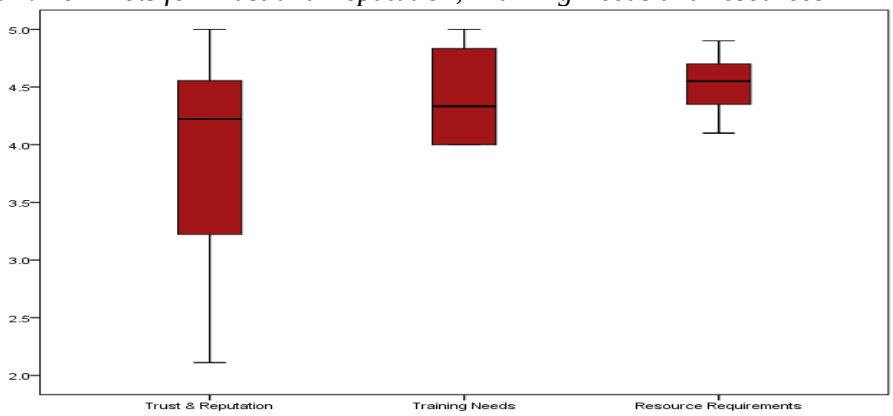
Table 1. *Descriptive Statistics for Constructs*

Construct	Mean (SD)	Median (Range)	IQR
Trust & Reputation	3.87 (0.81)	4.22 (2.89)	1.34
Training Needs	4.43 (0.41)	4.33 (1.00)	0.83
Resource Requirements	4.50 (0.21)	4.55 (0.80)	0.35

Note: *N = 63; Scale ranges from 1 (strongly disagree) to 5 (strongly agree).*
Source: *Authors' Compilation.*

This output revealed that the respondents reported (on average) high levels of trust towards financial services firms and their respective reputation following GDPR (Md = 4.22), yet the scores ranged from 2.55 to 5.00 suggesting high variability in scores across respondents; high levels of training needs following the GDPR, with scores ranging from 4.00 to 5.00, suggesting minimal variability in the scores among respondents; and high levels of resource requirements following the GDPR, with scores ranging from 4.10 to 4.90, suggesting minimal variability in the scores among respondents. The boxplots in Figure 1 display the data for the three construct measures graphically.

Figure 1. *Box Plots for Trust and Reputation, Training Needs and resources*



Source: *Authors' Compilation.*

Table 2 provides descriptive statistics for trust and reputation, training needs and resources by firm type following GDPR.

Table 2. *Descriptive Statistics for constructs by Firm Type*

Construct	Firm Type	Mean	Std. Dev	N
Trust & Reputation	Administrative	3.89	.69	31
	Customer Oriented	3.86	.93	32
	Total	3.87	.81	63
Training Needs	Administrative	4.42	.40	31
	Customer Oriented	4.43	.43	32
	Total	4.43	.41	63
Resource Requirements	Administrative	4.50	.21	31
	Customer Oriented	4.50	.22	32
	Total	4.50	.21	63

Source: *Authors' Compilation.*

The descriptive statistics in Table 2 reveal that the mean scores for trust and reputation, training needs, and internal policies, procedures and resource requirements were quite similar for administrative and customer-oriented firms.

The Levene's test was not significant for trust and reputation ($F(1,61) = 3.33$, $p = 0.073$), training needs ($F(1,61) = 1.02$, $p = 0.30$), and resource requirements ($F(1,61) = 0.14$, $p = 0.91$), implying that error variance of each dependent variable was equal across groups.

Furthermore, the Box test statistic was not significant ($M = 4.75$, $F(6, 2688.24) = 0.75$, $p = 0.61$) implying that the covariance matrices are roughly equal and hence the assumption of homogeneity of covariance matrices was tenable. Hence, we proceeded to interpret the Multivariate test statistics, which are exhibited in Table 3.

Table 3. *Multivariate Tests*[a]

Effect		Value	F	Hypothesis df	Error df	Sig.
Intercept	Pillai's Trace	.998	12788.826[b]	3	59	.000
	Wilks' Lambda	.002	12788.826[b]	3	59	.000
	Hotelling's Trace	650.279	12788.826[b]	3	59	.000
	Roy's Largest Root	650.279	12788.826[b]	3	59	.000
Firm Type	Pillai's Trace	.001	.023[b]	3	59	.995
	Wilks' Lambda	.999	.023[b]	3	59	.995
	Hotelling's Trace	.001	.023[b]	3	59	.995
	Roy's Largest Root	.001	.023[b]	3	59	.995

Design: Intercept + Firm Type; b. Exact statistic
Source: *Authors' Compilation.*

Table 3, shows that there was no significant effect of business type on trust and reputation, training needs and resource requirements, and this was confirmed by the four multivariate test statistics.

4.1 Thematic Analysis of Comments

Some participants (10%) noted further that although the GDPR has put increased pressure on resources, it is long outstanding since the older Data Protection Directive was not adequate to cater for changes we are faced with today. Some (8%), mainly from the insurance sector argued that this regulation came at the wrong time, given that they are already stretched as it is preparing for other regulations such as the Insurance Distribution Directive (IDD) and the new anti-money laundering (AML) implementing measures. Others (25%) mentioned that there are still some grey areas, which need to be clarified especially when conflicting with other regulations such as the AML requirements. Some (15%) mentioned, the lack of trained and knowledgeable Human resources to address the requirements.

5. Conclusion

The GDPR was a long waited requirement; it improves the relationship between the organisation and its data subjects, improves security standards and is a standardised regulation throughout the EU. By being compliant with GDPR, most of the organisations have seen that the level of trust towards the organisation has increased, since organisations are being more transparent and minimising the risk of data breaches.

However, although, its cons may outweigh the pros, the participants in the interviews argued that the GDPR has a lot of positive impacts. It is a drain on resources, costs and time. The GDPR is a huge overhaul from the previous Data Protection Directive and requires training and some organisations are still struggling to warrant compliance with the regulation. A take from this paper is that in drawing up regulations, regulators need to give more heed to small nations and understand better how the concept of proportionality can be applied more effectively. It has to be addressed without reducing the societal protections. That is the necessity of protecting the fundamental rights of a human subject. However, one needs to strike a balance between the means used and the intended aim. Specifically, proportionality requires that advantages are not outweighed by the disadvantages. That is without creating unnecessary burden on the smaller nations and organisations.

References:

Alshenqeeti, H. 2014. Interviewing as a Data Collection Method: A Critical Review. English Linguistics Research, 3(1).

Baldacchino, G. 2006. Islands, Island Studies. Island Studies Journal, Vol. 1, No. 1, 3-18.

Baker, J. & Lampaki, D.A. 2017. The Impact of GDPR on HR, s.l.: s.n.

Bezzina, F. and Grima, S. 2012. Exploring factors affecting the proper use of derivatives: an empirical study with active users and controllers of derivatives. Managerial Finance, Vol. 38, No. 4, 414-434.

Bezzina, F., Grima, S. & Mamo, J. 2014. Risk Management practices adopted by financial firms in Malta. Managerial Finance, (Emerald Group Publishing Ltd.) vol. 40, no. 6, 587-612.

Bishop, P.A. & Herron, R.L. 2015. Use and Misuse of the Likert Item Responses and Other Ordinal Measures. International Journal of Exercise Science, 8(3), 297-302.

Braun, V. & Clarke, V. 2006. Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77-101.

Brickendon Consulting Limited. 2018. Top Five Impacts of GDPR on Financial Services. Available at :https:// www.brickendon.com/articles/top-five-impacts-gdpr-financial-services/.

Briguglio, L. 1995. Small island developing states and their economic vulnerabilities. World Development, Vol. 23, No. 9, 1615-1632.

Carr, L.T. 1994. The strengths and weaknesses of quantitative and qualitative research: what method for nursing? Journal of Advanced Nursing, 20(4), 716-721.

Charoenruk, D.D., n.d. Communication Research Methodologies: Qualitative and Quantitative Methodology, s.l.: s.n.

Cookiebot, n.d. GDPR and cookies | What do I need to know? | Is my use of cookies compliant? Available at :https://www.cookiebot.com/en/gdpr-cookies/.

Deloitte Malta, n.d. Understanding GDPR: How will the Financial Services sector be affected? Availablbe at: https://www2.deloitte.com/mt/en/pages/risk/articles/mt-gdpr-fsi.html.

European Data Protection Supervisor, n.d. The History of the General Data Protection Regulation. Available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

European Parliament and Council. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, 38, 31-50.

European Parliament and the Council of the European Union, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, pp. 1-88.

Field, A. 2009. Discovering statistics using SPSS. 3rd Ed. SAGE. London, UK.

Fimin, M. 2018. Five Benefits GDPR Compliance Will Bring To Your Business. Available at: https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/#78e82dc0482f.

GDPR Report. 2017. GDPR: Guidelines and consequences for non-compliance. Available at: https://gdpr.report/news/2017/06/16/gdpr-guidelines-consequences-non-compliance/.

GDPR-Info, n.d. Right to data portability. Available at: https://gdpr-info.eu/art-20-gdpr/.

Hadabas, K. 2018. How will the GDPR affect human resources professionals? Available at: https://tresorit.com/blog/how-will-the-gdpr-affect-human-resources-professionals/.

Harris, L.R. & Brown, G.T.L. 2010. Mixing interview and questionnaire methods: Practical problems in aligning data. Practical Assessment. Research and Evaluation, 15(1), 1-19.

IdSurvey. 2018. Advantages and disadvantages of telephone interview surveys.

Available at: https://blog.idsurvey.com/en/advantages-and-disadvantages-of-telephone-interview-surveys/.

Irwin, L. 2018. How banks should prepare for theGDPR. Available at: https://www.itgovernance.eu/blog/en/how-banks-should-prepare-for-the-gdpr.

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

King, R. 1993. The geographical fascination of islands. In Lockhart, D.G., Drakakis-Smith, D. and Schembri, J. (Eds), The Development Process in Small Island States. Routledge, London, pp. 13-37.

Kotur, I. 2018. Your Guide to GDPR Compliance: Training your employees. Available at: https://platform.sh/blog/your-guide-to-gdpr-compliance-training-your-employees/.

Lautenschläger, S. 2017. Is small beautiful? Supervision, regulation and the size of banks. Speech at IMF seminar, Washington DC, 14 October.

Lilkov, D. 2018. The Impact of GDPR on Users and Business: The Good, The Bad and the Uncertain, s.l.: s.n.

Lord, N. 2018. What is the Data Protection Directive? The Predecessor to the GDPR. Available at: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr.

Lord, N. 2019. What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPRCompliancein 2019. Available at: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance.

McGavisk,T.n.d. ThePositiveandNegativeImplicationsofGDPR. Available at: https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr.

Miller, R.G. 1991. Simultaneous Statistical Inference, Springer-Verlag, New York, NY.

Mommers, L. 2018. Safe guarding your reputation under the GDPR. Available at: https://www.privacyperfect.com/en/blog/safeguarding-your-reputation-under-gdpr.

Naderifar, M., Goli, H. & Ghaljaie, F. 2017. Snowball Sampling: A Purposeful Method of Sampling in Qualitative. Strides in Development of Medical Education, 14(3).

Office of the Information and Data Protection Commissioner. 2018. Data Protection Guidelines for Banks, s.l.: s.n.

Remoortel, F.V. 2016. Financial institutions and the General Data Protection Regulation. Available at: https: www.financierworldwide.com/financial-institutions-and-the-general-data-protection-regulation/.

Rossow, A. 2018. The Birth of GDPR: What is it and What you Need to Know. Available at: https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#3e75892855e5.

Saunders, B. et al. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. Quality & Quantity, 52(4), 1893-1907.

Siegler, J. 2018. GDPR Industry Focus: How does the GDPR Impact Financial Services? Available at: https://www.logicgate.com/2018/02/21/gdpr-industry-focus-how-does-the-gdpr-impact-financial-services/.

Smith, M. 2017. The Limitations of Telephone Interviews. Available at: https://shortlister.com/limitations-telephone-interviews/.

Sullivan, G.M. & Artino, Jr.A.R. 2013. Analyzing and Interpreting Data From Likert-Type Scales. Journal of Graduate Medical Education, 5(4), 541-542.

The International Trade Administration. n.d. Privacy Shie Overview. Available at: https://www.privacyshield.gov/Program-Overview.

Tjalsma, R. 2017. An introduction to the General Data Protection Regulation. Availableat: https://www.workflowwise.com/blog/an-introduction-general-data-protection-regulation-gdpr.

Unisoft atatech Blog. 2016. The Importance of Data Processing to Your Business. Available at:https://www.unisoftdatatech.com/importance-data-processing-business/.

Wolf, E. 2018. GDPRand DataProtectionas a benefit. Availableat: https://www.businessbrew.io/blog/gdpr-and-data-rotection-as-a-benefit.

Wright, T. 2018. The GDPR– Is reputation a biggerrisk than fines? Available at: https://blogs.sas.com/content/datamanagement/2018/01/11/gdpr-reputation-bigger-risk-fines.

Appendix:

Interview Schedule

Section 1. Please select the nature of business that you work in.
Company Service Provider
Credit Institution
Financial Institution
Insurance
Audit Firm
Other: _____

Section 2: Please tick as appropriate
1-Strongly Disagree, 2- Disagree, 3 Neutral, 4 – Agree, 5- Strongly Agree

2. Theme 1: Trust and Reputation
The European Union wanted to increase the level of trust towards institutions, more precisely Financial Institutions. With the implementation of GDPR, the European Union hopes that institutions will regain some of the trust they may have lost due to past events.

○	The organisation aims to become a trusted holder of personal information, which in turn improves the long-lasting and loyal relationship with the data subject.
○	The organisation is seen as more reputable due to higher level of trust.
○	Putting into place data protection measures assists the organisation to be more accountable and trustworthy.
○	The process of requesting prior consent regarding cookie usage when a person enters into the organisation's website has increased transparency and trust.
○	The ability of a user to withdraw his/her consent regarding cookies at any time has increased transparency and trust.
○	When a data subject has given his/her consent that the organisation can contact him/her through various channels, such as by phone, mail, post or SMS, it can enhance data enrichment, which is a more dynamic approach in building a relationship with the data
○	If the organisation can show that it is more GDPR compliant than its competitors, it will show that it is a more reputable organisation.
○	With GDPR, marketing practices have improved, as tailored and effective campaigns focus more on customer engagement.

Q	The implementation of GDPR has reduced the number of complaints from customers.

Theme 2: Training needs, Internal Policies and Procedures

In order for employees to have a better understanding of the requirements of GDPR and its impacts on the organisation, the organisation has to organise and provide training with regards to data protection to its employees.

The Internal Policies and Procedures of an organisation have been affected by the General Data Protection Regulation. Policies and Procedures are designed to influence the designs and actions taken by the organisation's management.

Q10	The authorised staff responsible for the processing of personal data are given the appropriate training on data protection.
Q11	Training is provided to employees regarding the transfer of data to data subjects.
Q12	A culture of data protection by design that is embedded across all business areas requires extensive training.
Q13	GDPR has directly impacted data privacy and security standards while indirectly encouraging organisations to improve their procedures and policies on cybersecurity measures, limiting the risk of breaches.
Q14	Having a standardised set of data protection regulations means that if the organisation is GDPR compliant, it is free to operate throughout all European countries.
Q15	Access to critical personal data is limited to few employees thereby ensuring better data security and that data does not fall in the wrong hands.

Theme 3: Resources

For an organisation to be compliant with the GDPR and its requirements, the use of the organisation's resources will be very important. Financial, human, time, IT and software resources are all impacted throughout the various requirements of the GDPR.

Q16	With the introduction of the GDPR, the organisation will move towards improving its security by using new and evolving technologies that constantly monitor for data breaches.
Q17	The organisation is utilising its resources to focus solely on customers that are interested in engaging with the organisation.
Q18	The implementation of GDPR has improved data management because the organisation can remove any redundant files and make room for data that is actually needed.
Q19	The process time of requesting and acquiring data subjects' consent is increasing
Q20	The process time of informing data subjects as to why their data is being requested is increasing.
Q21	The process of keeping record of the risks involved and how these risks are mitigated is increasing.
Q22	The regular testing and updates on the Data Breach Incident Response Plan is increasing.
Q23	The process of ensuring that the information the organisation holds regarding data subjects is up-to-date is increasing.
Q24	Adopting data encryption and pseudonymous measures calls for constant surveillance to ensure that such practices prevent the organisation from being penalised and incurring additional costs.
Q25	The process time of deleting personal data after a valid request by a data subject is increasing.
Q26	The process time of sending data as requested by data subjects in a structured, commonly- used and readable format is increasing.
Q27	The appointment of a Data Protection Officer within the organisation incurs a financial burden on the organisation.
Q28	The organisation depends on the Data Protection Officer to adopt the new approach to privacy Regulation. There is need for a website structure, IT infrastructure and cybersecurity measures.
Q29	From a data protection perspective, selecting new vendor companies requires more scrutiny.
Q30	IT software and programmes offered by vendor companies need to be highly secured so that the probability of data loss is minimised
Q31	Personal data breaches add a 72 hour stress period whereby more human resources are needed to respond to a breach
Q32	If the organisation is not well prepared to protect personal

	data from breaches, loss or damange, the organisation will incur further costs due to penalties.
Q33	The organisation might find difficulty in monitoring data in real time without increasing Resourced
Q34	Having adequate contracts between data collections and data processors are costly and time consuming.
Q35	The process time of reviewing the organisation's privacy notices is increasing.

Section 3 Any Other Comments