19th August 2020

National College of Ireland

Gary Reeves

DATE: 19TH AUGUST 2020

ABSTRACT

The European Parliament approved the implementation of the General Data Protection Regulation (GDPR) on the 27th April 2016 based on the protection of the natural person with regard to the processing of personal data and on the free movement of such data (European Parliament Council, 2018).

This study investigates if there is a clear awareness and understanding of the risks, costs and obligations incumbent upon Irish organisations in order to remain or become compliant with the aforementioned GDPR regulation.

A sample of 110 people that are directly involved in Data Protection, Compliance, Human Resources, Business Owners or individuals who are responsible for data compliance in Irish companies were chosen to participate in an online survey based on the authors contact list of companies. The participants were chosen to give a broad indicative sample from 10 main industry sectors, for example, medical, pharmaceutical, services, legal, construction, retail & airline.

The questions asked focused on information on specific GDPR awareness, industry analysis of the survey pool, previous and future training on GDPR, which were all targeted towards hardcopy documentation within Irish organisations. The questions were grouped together into 6 separate groups or themes of questions which would indicate the answering participants industry sector, their personal awareness of GDPR, if hardcopy documentation was retained by the organisation and needed to be addressed, what training has been received by the participants regarding GDPR and if additional financial resources were required for the organisation to get compliant with GDPR and if there were any known data breaches within the organisation. The questions were further broken down into three (3) main themes, that being: GDPR awareness, Industry Sector and Training on GDPR.

The research study demonstrated that all participants, in their own opinion, had a prima facie basic understanding regarding GDPR compliance, with the largest percentage of respondents reporting they are very familiar with the regulations and a lesser amount having an increased awareness and being extremely familiar with GDPR compliance regulations. Based on the target audience of professional individuals specifically working or responsible for GDPR compliance, it was expected that there would be a higher percentage of respondents being extremely aware of the GDPR regulations. The results seem to be indicative of a lack of understanding, training, expertise, knowledge and willingness to comply fully to the GDPR regulations in place even with the enormous financial threats of fines that can be levied in certain circumstances by the Data Protection Commissioner of Ireland.

DECLARATION

Submission of Thesis and Dissertation

National College of Ireland
Research Students Declaration Form

Name: Gary Reeves

Student Number: 18145990

Degree for which thesis is submitted: MSc in Management

Title of Thesis:

A study to identify if there is a clear understanding and awareness of required records management policies and procedures in Irish Organisations, specifically, in relation to compliance with the General Data Protection Regulations (GDPR) which came into force on 28th May 2018.

Date: 19th August 2020

Material submitted for award

A. I declare that this work submitted has been composed by myself. ✓

B. I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged. ✓

C. I agree to my thesis being deposited in the NCI Library online open access repository NORMA. ✓

D. I declare that no material contained in the thesis has been used in any other submission for an academic award. ✓

Signed: 

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to my wife Claire and children for their continued support and understanding during the term of my studies and beyond.

I must extend my gratitude to my employer, the Senior Leadership Team and the Board of Directors who have believed in my ability by investing time and financial resources in me to make this educational program a reality.

My new friends in the National College of Ireland, the extended teaching faculty who I had the pleasure in meeting and of course Dr. Caoimhe Hannigan for your mentorship and guidance on the preparation of this dissertation.

Lastly, but certainly not least, to all the participants in my research, thank you so much as without your input none of this would have been possible.

CONTENTS

TITLE

A study to identify if there is a clear understanding and awareness of required records management policies and procedures in Irish Organisations, specifically, in relation to compliance with the General Data Protection Regulations (GDPR) which came into force on 28th May 2018.

Author: *Gary Reeves*

Award: *MSc in Management*

Submitted to: *National College of Ireland, August 2020.*

Word Count: *18,226*

LIST OF ABBREVIATIONS

- GDPR General Data Protection Regulations
- DPC Data Protection Commission
- DPO Data Protection Officer
- ROI Republic of Ireland
- EU European Union
- DPA Data Protection Act
- IT Information Technology
- IoT Internet of Things
- SAR Subject Access Right

INTRODUCTION

Data Protection is important to all companies, organisations, institutions and industries globally. The fundamental right to protect the personal data of every individual is paramount to avoid causing potentially great harm to the person or the organization. Unauthorised, careless or ignorant processing of data has the potential to cause harm in the forms of prejudice to an individual, issues in relation bank or medical information being used without permission or reputational damage to the organisation for the careless handling of the data (Sarap, 2019). New European Union regulations were agreed and accepted by all EU member states in the form of GDPR (general data protection regulations) in May 2018, which put a higher onus on organisations to implement data protection processes and practices internally for all types of data being collected, that being either softcopy information in electronic format or hardcopy data in the form of any type of paper or printed format. This study has investigated if organisations have taken the lead on implementation of strict data protection procedures regarding existing hardcopy documents and practices in relation to future documentation retention.

The questions posed were designed to investigate how they have carried out such remedies, in terms of, have they put satisfactory knowledge in place with data protection training to the responsible individuals and if the general users are aware of their obligations in terms of data protection. Furthermore, if individuals within organisations are confident that they have received the correct training on GDPR and if they fully understand the potential risks to the company for data breaches of any kind.

In 1970 the internet first successfully linked 2 major companies in the USA, and was quickly followed in 1971 with the design of what we still use as ‘email’ today, then on to 1973 when the first trans-Atlantic internet connection was established (Craig, 2010). Over the past 30 plus years there have been many suggestions of the removal of the need for paper documents, and we are still awaiting the so-called ‘paperless office’. Although there have been many technological advancements across the generations when it was widely thought that computers would remove the necessity for paper files and filing cabinets,

we are no closer to a paperless office than we were back in the 80's (Millaken, 2014).

Email and the internet were thought to be the new technological advancement that would give access to all documentation, notes, data and information at the touch of a button, but in reality, this is not the case. There has most definitely been an increased ability to access documentation from anywhere in the world via cloud computing technology (Liu, 2019), but many people still prefer to print hardcopy records, emails and notes just to have the physical aspect of paper to read and write upon. The Mopria Alliance was founded in 2013 by the large print organisations at the time, namely, Canon, HP, Xerox and Samsung to set standards and solutions within printing universally. According to a survey carried out in 2019, it was reported 80.5% of workers enjoy the 'feel' of pen and paper, and 60% still prefer to take notes on paper as opposed to laptops or phones (Facility Executive , 2019). With up to 88% of people indicating they understood information from printed material, as opposed to 64% when reading from an electronic source (Printing Impressions, 2015).

All organisations generate hardcopy paperwork, some of which contains personal data and other paperwork that must be retained for a certain timeframe for normal business and compliance reasons. The variety of hardcopy documents and records generated begins with the initial creation of the company and subsequent registration with the Companies Registration Office (CRO). The CRO provide registration forms in PDF format for submission in hardcopy format (www.cro.ie, 2019) [Appendix 1], and this trend continues through the life of any organisation with the receipt (and printing) of emails, patient records, bank statements, cheques sent & received, application forms, human resource forms and client details, to name just a few. There is now intense public awareness and attention surrounding GDPR changes and about data privacy issues like never before (Bauer, 2019). Therefore, not only is it incumbent on organisations to be prudent and secure with personal data recorded, it is a legal requirement.

According to a survey completed jointly by McCann Fitzgerald and Mazars (Lavery & McKenna, 2018) 88% of Irish Organisations surveyed believe they

have interpreted their GDPR obligations correctly, however, it was found that 64% found it challenging to create the structures necessary for data protection compliance. The research undertaken will identify any known or obvious reasons if there are challenges in creating a culture of compliance within organisations and if the previous research around GDPR compliance has changed in any way in 2020. The research will look at awareness from a personal perspective of the main users, controllers, and participants with regards to hardcopy documentation compliance within Irish organisations and whether the organizational perspective on awareness is the same as the individual's perspective.

12 months on from the implementation of GDPR in Ireland it is suggested above in the McCann Fitzgerald & Mazars published survey that businesses are struggling to put in place what is required to protect the company in relation to data protection, which could indicate that training and awareness are not as robust and accessible as they are believed to be. The author will highlight available literature and articles relating to these issues, moreover, the author will offer evidence of the actual awareness of the survey participants as to their understanding of GDPR and if further investment may be needed to ensure appropriate expert awareness is achieved.

The research was conducted on a list of participants that are involved in a variety of different organisations, different industries and industry sizes to see if there is any correlation in results relating to the questions asked regarding awareness of GDPR in their respective organisations. This was done using an online survey questionnaire and asked specific questions relating to six (6) areas sub-headings that would give a matrix of results to quantify the conclusions being made. The sub-headings were devised to cover industry, industry size, existing hardcopy documents pre-GDPR, existing retention policies, awareness of any data breaches that may have already occurred and finally the quantity and location of the existing hardcopy records for the company. The participants were asked to acknowledge their agreement to participate and continue in the survey and could have decided not to continue at any time. No personal data relating to the survey participants were recorded or retained at any time.

CHAPTER 1 – LITERATURE REVIEW

1.1 INTRODUCTION

GDPR is here to stay and will change the way businesses view and handle personal data forever. Since the implementation of GDPR in May 2018 the various EU member states have given increased powers to their respective Data Protection Offices, for example, large financial penalties and personal director liabilities, along with organizational reputational damage. These increased powers should not be taken lightly as in most cases the Data Protection Office can now publish Court successes on their websites naming the offending companies, even if the financial penalties are affordable, the negative publicity around any GDPR data breaches are much harder to absorb (GDPR Associates , 2019). The research will identify & discuss various reports and studies completed in relation to GDPR compliance, data breaches, training given, training received, and implementation plans for organisations.

As the study is focusing on hardcopy records management, the investigation into the IT sector will be limited to sources of existing reported data breaches to the Data Protection Commission and any relevant fines issued for comparative purposes only. For example, a report published by the Journal of Internet Law gives some brief comparative details and highlights the extent of the challenge within the IT sector due to the rapid growth in what is termed the Internet of Things (Iot) and the fact that there were reported to be in excess of 8.4billion connected devices worldwide in 2017 which shows the growing challenges within the IT industry regarding data protection (Kearney, 2019).

And additionally shown in a survey conducted by the Irish Computer Society (ICS) that more than 22% of IT administrators surveyed have had multiple data breaches in the last 12 month period, with 51% reporting a breach of some kind in the same period, which is a sharp rise from the previous year (ICS, 2019).

In line with the understanding of the author of this piece of research and the choice to focus on hard copy documentation only within Irish organisations

(Pinto, 2018) backed this up by commenting that studies into E-Privacy requirements and potential hacks, pitfalls or data breaches would have to be completed in a separate study in singularity.

While there is an abundance of literature available regarding GDPR regulations, there is no current supporting literature solely based around the challenges in dealing with hardcopy paper documentation or records specifically in relation to Irish Organisations.

We will begin this piece of research by detailing the actual right to privacy for individuals within Ireland that could be impacted by a data breach of any organisation holding sensitive information or personal data of any individual.

1.2 RIGHT TO PRIVACY IN IRELAND

In accordance with Article 40.3 of the Irish Constitution every citizen of Ireland has the right to privacy engrained as one of their unenumerated rights which extends to personal data relating to any individual who can be identified form that data in the form of electronic or manual files (www.gov.ie, 2020). The European Convention of Human Rights further backs this up stating that everyone has the right to respect for their private and family life, their home and their correspondence, which is stated in Article 8 of said Convention enshrining each person's rights further (www.iccl.ie, 2019).

It is helpful to understand what is meant when we talk about privacy, there are different connotations of privacy including the territorial privacy based on property, privacy of the person relating to a physical space, freedom from surveillance & harassment, right to be left alone and privacy in the information context which is based on the assumption that all information about a person is their own and they may disclose this information in certain circumstances and when they do disclose this information it must be protected from unapproved usage or dissemination (The Law Reform Commission , 1998). Irish Law places great emphasis on human dignity and strongly supports a right to privacy, however, there is no specific directly written right to privacy within the Irish Constitution. However, there is an assumed right to privacy for all

individuals under an assumed or implied recognition of this by the Irish Courts (Citizens Information , 2019).

There is an assumed right to privacy with regards to private written correspondence or private telephone conversations which cannot be deliberately interfered with, however this of course may be restricted in the interests of the common good (Citizens Information , 2018). In 2014 a high profile case in the Irish Courts was closely watched by interested parties as the judge tried to balance the strong constitutional right of privacy of a birth mother, with the rights of adopted children to know their birth parents (O'Halloran, 2014). Which resulted in the introduction of the Adoption Amendment Act 2017, that put the best interest and rights of the child to the forefront, if the child wants it, which in this case puts aside the right to privacy in the case of the mother involved.

1.3 DATA PROTECTION ACT

In 2018 the European parliament approved the implementation of the GDPR regulations for all member states (European Parliament Council, 2018), see Table 1 in appendices (page 69), however, prior to this implementation there were already existing rigorous Irish Data Protection regulations detailing how organisations that collect personal data should manage said data, giving explicit definitions of personal data and how this should be protected (Data Protection Commission , 2020). The protection of the data is written into law under the Data Protection Acts 1988 and 2003, as well as a 1995 directive, but is now strengthened under the new regulations since May 2018. (Data Protection Commission , 2020). It is important to note that all references to data mentioned above covers any personal data in both electronic and hardcopy format.

As per a report by Leo Moore from William Fry Law Firm, in Ireland the Data Protection Act 2018 was formally passed into legislation on 24th May 2018, just in time for the implementation of the European Union GDPR act which came into effect on the 25th May (Moore, 2018). The acceptance of the GDPR act within the EU member states was combined together with the Data Protection

Act 2018 (DPA) in Ireland to strengthen the powers of the Data Protection Commissioner (DPC) which had a seminal influence on the topic being researched.

The inclusion and combination of the GDPR act with the pre-existing Data Protection Act brought about the following significant changes:

- The DPC now has the ability to issue fines to organisations
- The DPC has greater investigative powers, including the ability to apply and act on search warrants
- The DPC can request the High Court to suspend all data processing activity on any organisation if there is an urgent need to do so
- The age of digital consent was raised from 13 to 16 years of age
- It is now an offence for a company to process the personal data of a child (under 16) for the purposes of direct marketing, profiling, or micro targeting (Shannon, 2018).
- Company officers or directors may be held criminally liable for data breaches if they have failed to do something that was expected of them in terms of compliance, even if they have no actual knowledge of the offence (Reynolds, 2018)

Data can flow freely and unhindered between the member states of the European Union, across all borders to and from Ireland, making business faster and easier in many cases. Which the introduction of GDPR within the European Union means all Irish organisations must comply. However, although GDPR gives member states limited scope to apply the Regulation within their own country, this also means that the data protection laws must be robust to protect any EU citizens data if shared with Irish organisations (Data Protection Office, 2018).

The Data Protection Act of 2018 was accepted into the Irish Statute books which enhanced the powers of the Data Protection Commissioner in accordance with the European Parliament and of the Council of 2016 to bring Regulation (EU) 2016/679 with regards to the processing of personal data and the protection of natural persons and their personal data (Irish Statute Book,

2018). The European Union implemented the agreed and accepted GDPR Act 2018, which outlines the protection of the data of the natural persons in Ireland, however, the EU GDPR regulation does not impose criminal sanctions directly on companies that may be classed as a data controller* of this information for any breaches or contraventions, the penalties for this are left to the member states to decide which was covered in the Irish Government Data Protection Bill of 2018. (Brennan, 2018). Some of the corrective actions that the Data Protection Commissioner can apply to any organisations could be as follows:

1. Warnings or reprimands
2. Temporary or permanent ban on data processing
3. Up to €20million or 4% of the company's annual gross turnover

(I.T Governance , 2020)

** data controllers are those who take any part in obtaining, recording, keeping storing, destroying, organizing, combining, or disclosing any sensitive personal data, these can be any legal entities or government depts.*

1.4 PERSONAL DATA AND THE PUBLIC

All organisations generate paperwork, some of which contains personal data and other paperwork which must be retained for a certain timeframe for business compliance reasons. The introduction of GDPR in May 2018 has heightened public awareness about data privacy issues (Bauer, 2019). Under Article 15 of the GDPR regulation (DPC, 2019) individuals have the right to request access to of any of their personal data which is being processed (used in any way) by anyone who decides how and why the data is being processed. The request must be responded to within one (1) month of the original request (DPC,

"Before I write my name on the board, I'll need to know how you're planning to use that data."

2019), which could put pressure on organisations to have correct identification, retrieval and response systems in place in order to provide this information within the required timeframe. Therefore, organisations must be aware of what data they are recording, retaining, why they are retaining it and be in a position to provide this same information to anyone requesting visibility of their data in question. In addition to data given to companies by the person on various forms of application etc..... many companies collect data on the individuals behaviour, location, shopping, and online searches to gain what they would deem as valuable consumer trends and insights into the potential buyer market. In fact, there are companies that have been set up with a business model entirely around consumer data capturing, with the intent to build targeted advertisements to the consumers or to sell the information to another 3rd party company so they can use the information for targeted business purposes – simple fact is that customer data is big business (Uzialko, 2018). Businesses and organisations that collect consumer data also fall under the GDPR regulations of 2018 and must protect the rights of the individual at all times aswell, the question must be asked that if businesses are gathering this consumer information and using it for targeted adverts or selling the information on to another organisation does the individual need to consent? Have the individuals consented in some format unknowingly? Under GDPR regulations, any organisation that an individual signs up to or registers an interest or uses their app or social media site must use what is termed as a 'click wrap' registration that the individual must click a check box or linked button to accept the terms & conditions of the organisation, and make it available to the individual in an easily viewed format the individual can view anytime (Termsfeed, 2020). A Deloitte survey in the United States was carried out on 2,000 individuals and subsequently reported that 91% of respondents never read the terms and conditions, which increases to 97% for individuals that are aged between 18-34 years. Consumers that wish to access a program, IT application, game or software are sometimes faced with no choice but to accept in order to gain access do so without knowing the consequences or what they are agreeing to (Cakebread, 2019).

According to the Information Commissioners Office (ICO) in the United Kingdom, there has been a sharp increase in the public's awareness of their data protection rights which is evident by an increase of 14.5% of data protection complaints over the past 12 months from July 2017 to July 2018, which includes the implementation of GDPR (Afifi-Sabet, 2018). This increase in awareness which has led to reporting of data privacy complaints has also been witnessed in Ireland, with an increase of 75% of cases reported to the Data Protection Office in 2019, totaling 7,215 cases reported in the previous 12 months (Data Protection Commission , 2019).

1.5 DATA BREACHES, RISKS AND POTENTIAL COSTS

There was a sharp rise in the number of data breach reports in Ireland which was reported in the Data Protection Commissioners 2019 report, which highlighted an increase in the first full calendar year of the GDPR regulation implementation in Ireland. The figures rose from 4,113 complaints in 2018 up to 7,215 complaints in 2019 showing an increase of 75% of complaints (Data Protection Commission , 2019).

The figures given here are relating to data breaches that were officially reported through the correct channels.

In 2019, Ireland reported 6,716 data breaches to the Data Protection Commissioner with a population total of nearly 5million people, in vast contrast to Italy who reported 1,886 data breaches with a population of around 60 million people, suggesting 'cultural differences' in reporting of breach notifications need to be taken into account if comparing countries (Gorey, 2020).

It is imperative that Irish organisations do not take their eye off the ball at any time and must remain vigilant in this regard, for example, there were 41 reported data breaches of sensitive information in 2018 within the Irish **Justice Department** (McDonagh, 2019).

Some Key Data Breach Statistics in Ireland are as follows:

€56,000,000 in fines to end of December 2018

91 fines have been handed down in total

4,113 complaints have been received in Ireland during 2018, up 56% year on year

There were more complaints lodged between 28th May 2018 and end of November than in the whole of 2017

In the UK, between 28th May 2018 and end of October 2018, data protection related cases increased by 133% over the same period in 2017

*Source: (*Doyle, 2019)

There are significant risks and costs to the organisation pertaining to non-compliance and failure to implement adequate safeguards to combat against breaching data privacy laws. Through the Data Protection Commission, GDPR regulations can allow for fines of up to €20million or 4% of any organisations annual turnover, so the risks are extremely high (McGuone, 2018). In fact, during 2019, the Irish Times newspaper reported that the tech giant Google has been fined €50 million for breaking European Privacy (EU) laws (The Irish Times, 2019), which is greatly increased from the Irish maximum fine of €20 million.

Due to the low corporate tax rate in Ireland at 12.5%, Ireland have attracted the large technology companies like Facebook, Microsoft, Apple, Twitter and Google to set up headquarters in Ireland. According to a report by Focus Magazine, the Data Protection Controller, Helen Dixon, stated in early 2019 that she expected to receive an estimated 10,000 data breach complaints in 2019 and will have no hesitation in investigating these larger technology based organisations (Mayer, 2019). These companies are the high-profile, low hanging fruit, that can be identified and penalized as required, however, the question should be asked - how long will it take for all organisations no matter the size to be reviewed in the same manner?

To date there have been some massive data breach fines levied on various organisations, mainly in the IT sector or high-profile companies throughout the UK, USA and globally. In fact, the fines being assessed for issue are of such proportions suggest that the regulators in the various countries are beginning to get more serious about data protection of consumer data. For example, British Airways were imposed with a $230million penalty, The Marriott Hotel chain with a $124 million fine and Equifax in the USA agreed to pay $575 million for its data breach in 2017 (Tech Central , 2019). To date, most higher valued fines have been in relation to electronic customer data being hacked, stolen, lost or otherwise misappropriated, but firms that control or process personal data in hardcopy documentation format need to be aware and diligent at all times to avoid penalties and also reputational damage accordingly. A study in the USA by Centrify reported that 65% of victims of a data breach lost trust in the organisation as a direct result of that breach, and more worryingly, that 80% of consumers will stop using a business if their information is compromised (Hospelhorn, 2020). Therefore, companies should take seriously the potential of any breach of data that may result in loss of trust with the consumer, leading to negative word of mouth publicity and subsequent growing reputational damage.

In Ireland one of the most hardcopy document reliant industries would be the medical sector (hospitals) as they have generated paperwork for every patient, every visit, every procedure, and every death since the beginning of note taking. Many of which are stored externally in records management companies providing professional document retention & retrieval services. In the authors organisation alone, there are in excess of 65million hardcopy medical records alone ranging from births, x-rays, visits, surgeries, A&E charts and records of deaths of Irish nationals and visitors alike.

While looking at these numbers you would expect the hospitals to have steadfast data protection procedures and guidelines, but there have been multiple instances of medical records being found outside of the hospital's protection. In 2018 Mayo University Hospital had to publicly apologise for patient charts being found in a refuse sack in a housing estate by County Council workers (Shiel, 2018). The Independent newspaper reported that

patient records were found in a pub that should have been in Letterkenny University Hospital and lost medical files containing patient details turned up on a bus in Waterford in 2019 (McDonagh, 2019), plus the fact that the HSE have reported 465 incidents of breaches containing sensitive personal data in 2019. Other hospitals being reported for similar sensitive material breaches are Our Lady's of Lourdes Hospital in Drogheda (4 x incidents), St. Luke's Hospital in Kilkenny, Galway Mental Health Services, University Hospital Galway, University Hospital Waterford and Connolly Hospital in Dublin (McDonagh, 2019).

Data breaches are never 100% avoidable, even with robust data protection processes and procedures you can never fully mitigate for human error (Data Conversion, 2019), for example, a message that was meant to be sent to Jon and went to John instead could have serious consequences. It has been suggested that company executives believe that their organisation has been subject to an internal accidental data breach in the last five years and 44% of them believe they happen when using company email (Pepper, 2020).

When human beings are involved, human error can happen to even the most experienced and well-trained person. Human error can occur in the form of skill based errors or mistakes (Health Service Executive, 2020), but the important thing is how you deal with it afterwards. A comprehensive report on the root cause, the corrective actions and the implementation of new procedures are crucial to trying to stop the same mistake happening again and the focus should be on the process and not on the person with trying to identify the error link in the process (Lush, 2019).

The Data Protection Commission require all breaches containing personal data to be reported within 72 hours (DPC, 2019), but there is doubt whether this is actually what happens as organisations may not want the negative publicity that possibly goes with the case and that loss of market share due to loss of client trust which could be carried over to future customers is more than likely to be the biggest price any organisation will suffer due to data breaches and subsequent reporting (McElhill, 2019). Another European example of

companies not reporting data breaches is the case of MisterTango UAB, who failed to report a significant data breach when it allowed a list of payments to be publicly visible on its website before correcting the error. The company, which was based in Lithuania was fined €61,000 for not filing the report within the required 72 hour rules in GDPR and breached Articles 5, 32 and 33 accordingly (European Data Protection Board, 2019).

On the 18th May 2020, nearly 2 years on since the implementation of GDPR into Irish regulations, the Irish Data Protection Commission passed their first fine within the State to the Irish governments Child and Family agency, called TUSLA, for failing to adequately protect the information regarding 3 children were the information was wrongly disclosed to a third party. The agency was fined €75,000 following this investigation (Nathan Trust , 2020). Although, this may be seen as a breakthrough in Irish implementation and follow up investigations, the fine levied pales in significance to an example in The Netherlands where a fine of €725,000 was levied against a company that recorded the employees fingerprints on a time-in-attendance system where the company was found not to have established a fair legal basis on the grounds for the use of the data being recorded (Nathan Trust , 2020).

1.6 RETENTION PERIODS

It should be clear or made clear to organisations, data controllers and data processors that the 2018 GDPR regulation does not specify retention periods for personal data and only advises that this data should be *"...retained for as long as necessary"* for the purposes for which it was received and processed. (Dunne, 2018). Therefore, it is the organisations responsibility to decide what data should be retained, in what format, for how long, how this will be dealt with accordingly when it has expired its retention period and with supporting retention policies to ensure compliance throughout the organisation.

Sectoral advice on retention periods have been given in many industries, for example the Law Society of Ireland have issued guidelines for their members information, which on the face seem to be quite concise and useable, however, there is a caveat within the body of the report that these are for guidelines

purposes only and are developed with the writers own experiences (Technology Committee , 2018) *[Appendix 3].* Alternatively, within the education industry there seems to be a good comprehensive indication of what document retention periods should be, for example, Trinity College Dublin have a publicly available listing demonstrating these (Secretary to the College , 2016). *[Appendix 4].* The National College of Ireland also have a publicly available Information Governance handbook available which covers the advised retention periods for various record types (National College of Ireland, 2018) *[Appendix 5].*

Not only do organisations need to be prudent in collecting, retaining, storing, and dealing with personal data for persons they receive information from, organisations have internal documentation that also always needs the same careful consideration. For example, all organisations are required to retain human resource records, training records and hence very personal information regarding their own internal staff, such as home details, salary rates, sick notes relating to absences etc... Employees also always have the same rights for their information to be completely protected and not disclosed unless approval is given to do so. During the retention of this information it must be clear why this information is being retained and for what period, and the employee may also ask to review their full internal details at any time with no prejudice or delay. This is termed a 'subject access right' (SAR). Under GDPR all organisations must provide the full response with details within 40 calendar days or as soon as possible before that (Bolger, 2018). This should have an impact on how organisation conduct their internal documentation retention, either electronic or hardcopy formats to ensure full compliance and ensuring correct data destruction is carried out when it is no longer deemed as necessary to retain to continue with the persons employment.

The retention guidelines per industry should be observed and studied carefully by the responsible person relating the patient records. The Health Service Executive (HSE) have published a guide to retention period for various classifications of hospital records, they range from 2 years for cause of death records, to 5 years for clinic audit forms, to 8 years, 20 years, 30 years from last entry to a chart and much more complicated recording required to ensure the record is maintained correctly for the period advised, and in some cases to be

kept in perpetuity for child welfare records. [*See Appendix 6 below*] This is a mine field to manage, understand and retain compliance throughout the life span of the record and the career span of the data controller in the relevant hospital. Therefore, it is recommended by the Data Protection Commissioner that chart / record tracking systems need to be updated in many hospitals to electronic internal and external tracking systems and not continue to operate the manual operated systems in place to protect and record the whereabouts of patient data (Data Protection Commissioner , 2018).

Other industry recommendations include The Grand Hotel operating within the hospitality industry guidelines, which recommend retention periods ranging from 1 year for certain items to permanent retention of pension scheme records (The Grand Hotel , 2018). From reviewing the above documents on retention in the various industries there seems to be a recurring theme of a mean of 6 years for items in certain brackets, rising to permanent retention for other documents. The author won't discuss these in more detail as they are not relevant to the study, however the relevance being that the vast myriad of details to manage records that may contain personal data is indeed going to be a challenge for any individuals and organisations to be aware of and to comply with regulations.

1.7 TRAINING AND RESPONSIBILITIES

Training in the correct manner, forum and from an experienced individual is key to gaining awareness and knowledge for any skillset, system or process required to be carried out by an individual in an organisation. Business training is not just an important part of any company, it is critical, and even though the cost of training may sometimes seems expensive, the overall return on investment from training and development of employees is a no-brainer (London Business Training & Consulting, 2020).

The Irish Computer Society published an article relating to a survey by the Data Protection Commission in Ireland in which it was reported that nearly half of Irish companies are poorly trained for data breaches and that the biggest threat to Irish companies remains as negligent staff, with 20% of the companies surveyed stating that clumsy or lack of skills being the biggest threat to keeping

data secure (Irish Computer Society, 2020). However, one must be mindful of the method of training employed even though Internal training can identify the specific skills for the roles within the organisation and prepares individuals for succession within the company should the opportunity arise (Heathfield, 2020). The provision of professional external training should be considered in all cases.

Following on from internal training, we will now look into the provision of suitable external training with the main benefit of external professional training being that it is delivered in an impartial manner to all attendees and is given in a structured taught manner to gain the most effective outcomes. External training also can be seen as more effective as they are skilled trainers which understand and utilize specific training methods to captivate the audience and deliver the content in a focused manner which can provide a new 3rd party look at the process and challenges, while keeping focused at the job at hand (Woodman, 2019). The downside is of course that external training can be expensive depending on the training required, the trainer or company selected and other additional factors, like travel and other expenses. Wherever possible, high quality external training should be provided which can also give your staff recognizable qualifications in the field (Troy, 2017).

All employees must understand a basic level of GDPR and the associated risks to the organisation for any data breaches incurred, either by error or otherwise. Face to face training allows questions (and answers) on a more personal and direct level, but don't over complicate it and it is vitally important that all staff should at the very least understand what is meant by personal data, how the company uses the data and how they themselves in their roles in the company use the data (Natwest Bank , 2020). Bear in mind, that depending on the persons role in the organisation the level of training and understanding will need to be adjusted, for example, the person at the reception desk may need a rudimentary understanding of the principles of GDPR, as opposed to the team in the Human Resource department, the Records Manager or Data Controller who will need quite in depth understanding of the regulations.

Since the inception of GDPR in 2016, there have been numerous amounts of private organisations, or consultants established or diverted to provide direct GDPR training for organisations staff and individuals alike. In 2019, Fintan Swanton, the Chairman of the Association of Data Protection Officers indicated in an article with the Irish Computer Society that there is a need for Irish organisations to take further steps to manage their data processes more effectively as there are only moderate levels of awareness and training within Irish companies (ICS, 2019). In 2018, Helen Quinn of the Small Firms association published an article in the Veterinary Ireland Journal highlighting the need for veterinarians to be aware and concentrate on training practice members on GDPR compliance, offering six key areas for review (Quinn, 2016), which shows the complete spectrum of organisations that need to be aware, train and comply to the GDPR regulations.

Helen Dixon of the Data Protection Commission "has emphasized that GDPR is a 'front room to boardroom' process, and all frontline staff must be made aware of and trained in GDPR" (Quinn, 2018).

There are a vast amount of variations and offerings of training in relation to GDPR awareness with companies offering online training from the United States at a price range from $1,495 - $3,995 (International Association of Privacy Professionals (IAPP), 2019) to a very simple Irish online course provided at a cost of €25 per person (IACT, 2019), with a multitude of offerings in between including consultancy, onsite training and so on. There are 1 day professional training courses that can be taken through the Association of Data Protection Officers in Ireland which start at €595 per person (Association of Data Protection Officers, 2020), plus 3 day course which will give the participant a qualification in Certified Data Protection Practitioner Certificate (CDPP), followed by a more rigorous 6 day course which will qualify the individual as a European Certified Data Protection Officer (ECDPO). The investment required into these courses can suit all pockets and financial situations, however the company needs to be vigilant in providing the relevant and meaningful training to their employees that is relevant to the organisations requirements, industry, availability and financial resources and ensuring that the final outcome gives the

appropriate cover by being awarded an ISO 17024-certificated EU GDPR Foundation (EU GDPR F) qualification.

According to a survey completed by Mazars and McCann Fitzgerald (McKenna & Lavery, 2018) 58% of businesses surveyed estimate their GDPR related costs to date were between €50,000 - €250,000. Therefore, the financial and human resources should not be under-estimated and need detailed consideration.

In addition to the Irish based survey above, Deloitte UK carried out a GDPR specific survey moving outside the European Union for a more global view of the GDPR regulatory environment, in November 2018 Deloitte (UK) carried out a survey across eleven (11) countries both inside and outside of the EU across both consumers and organisations in these countries. The survey has shown some interesting findings, mainly that consumers are certainly more aware of their right to privacy and 58% of respondents take more care when providing personal information to organisations. Along with this the survey shows the organisations have already began to make significant investments in their compliance goals, with 48% reporting that they have done so in the last six (6) months since GDPR implementation (Deloitte LLP, 2018) [Appendix 8]. Part of the survey investigated what organisations have invested in additional human resources to become or to retain their GDPR compliance, the results showed that 99% of Indian companies had appointed a Data Protection Officer (DPO), the United Kingdom reported 92% have made new appointments in this regard and also 92% of Italian organisations, with the conclusion that these reported results are high numbers seen and are based on the high level of seniority that the organisations now place on accountability for data privacy.

In February 2018, just before the implementation of GDPR compliance, Ipsos MORI in Scotland were commissioned to undertake a survey of businesses in the United Kingdom by the Scottish Law Firm, Brodies. The results showed that at this late stage so close to implementation, only 70% of organisations were aware of their GDPR abilities at the time, but 25% of them were not aware at all. This was followed with a reported 72% of organisations stating they will be compliant by the 25th May 2018, and 11% admitting they will not be ready (plus

17% saying they do not know). The biggest challenges that they see in their ability to be compliant with GDPR are resources (human and financial) and cultural changes and lack of regulatory guidance (Brodies Law Firm, 2018) [Appendix 9].

1.8 CONCLUSION

Based on the details above there is obviously a lot of information available for any person(s) to investigate and review about GDPR training, regulations, articles and information, however, the information that is available is as suggested reliant on the individual to teach themselves as there seems to be no immediate evidence that all businesses are carrying out their responsibilities to the extent required. According to GDPR regulations there are significant fines that could be levied on the business for failure to be compliant at all times and it certainly seems that this type of information is certainly at the forefront of the reasons why any action is being taken at all. There are vast resources available for organisations to avail of the training required to keep the relevant company compliant, but there are also costs involved to do this to the correct standards, so the question being asked is; is this happening? There is clear evidence that many organisations have data retention policies in place, which many make publicly available to external users, plus various industry regulatory bodies offer guidelines on retention policies aswell, so this research will attempt to identify if the retention policies are understood by the organisations, but more importantly by the person(s) responsible for implementation. As many high-profile data breaches mentioned are in relation to well-known home brand technology companies and any 'hacking' or breach of data have been publicized, the attention is therefore directed towards electronic data. There does not seem to be any previous research completed in relation to GDPR regulations related to hardcopy documentation within Irish organisations which is the reason the author is attempting to fill this gap with the research study being investigated, and is more than likely because the GDPR regulations were only implemented in May 2018 and the evidence has not had the time to flow through the system, until now.

CHAPTER 2 – RESEARCH & AIMS

2.1 RESEARCH QUESTION

This paper is an investigation and analysis to identify if there is clear understanding and awareness by the responsible person(s) in Irish organisations regarding the risks and costs in relation to records management policies and procedures within Irish organisations in relation to compliance with the General Data Protection Regulations (GDPR) which came into force on 28th May 2018 in Ireland (Data Protection Commission , 2020). The investigation has been designed to show a personal level of understanding and awareness of GDPR regulations and where the participant personally ranks their awareness or knowledge of GDPR and how they have been trained in this subject matter. The research questions will be aimed towards people that are currently working in some regard with handling, organizing, storing, or managing hardcopy documentation in Irish organisations that contain personal or confidential data. The intended participants have been chosen because of the requirement in their business roles to understand GDPR regulations and to act in accordance with the regulations to achieve compliance within their organisation, which will include business owners, managers, data protection officers, compliance personnel and internal users of confidential material.

2.2 AIM OF RESEARCH

The aim of the research is to gather information that will demonstrate if the level of training and awareness of GDPR is of sufficient standard within Irish organisations that would allow them to claim they are compliant with GDPR regulations regarding hardcopy documentation. Specifically relating to documentation that contains any individual's personal data in hardcopy format that could potentially lead to a data breach if not conducted correctly.

Using a positivist approach (Science Direct, 2019) to analyse the research indicators, the results will attempt to further distinguish if the level of compliance is related to specific industries and make conclusions to the potential reasons for this. This study will also further investigate the type of training offered or

received by the participants to enhance their knowledge of GDPR and if there have been any financial investments into the training and achievement of GDPR compliance, or indeed what is required in the future to achieve this status or increase the knowledge base.

The author tries to demonstrate that there is a positive belief that the levels of awareness are good with most participants, however there is a lack of investment and professional training given to support and invest in this very important area of expertise that all organisations require, especially in relation to the targeted participants who are deemed the responsible persons regarding the compliance of hardcopy documentation within their respective organisations.

The research investigates if the sector that the organisation is within would also have an impact on the awareness within the organisation. Which may be due to the increased volume of documentation that would be reflective of the organisation itself which has the knock-on effect of requiring a more considered approach to GDPR and data compliance. It is also believed that there is a possible correlation between GDPR awareness being fully understood and the financial investments made by the company into this very important area of compliance, including investing in external training, putting the correct amount of human resources in place and doing so on a continuous basis. The results are analysed and the findings will indicate the conclusions and discussion points on each question noted below.

CHAPTER 3 – METHODOLOGY

3.1 INTRODUCTION

In this chapter, we will detail and discuss the methodology used to collate the responses required that will give indicators for discussion and lead to an answer to the question detailed in the previous chapter.

Suitable participants were identified by the author based on their roles and responsibilities within an organisation, namely persons, managers or business owners that are responsible for ensuring compliance within their relevant company in terms of GDPR and specifically relating to hardcopy documentation. Each participant was emailed directly with an online survey of 26 questions relating to hardcopy documentation and GDPR awareness, at any stage during the survey the participant could opt out and not proceed any further. The survey was sent to 110 respondents in total, with a response total of 95 completed surveys.

3.2 RESEARCH DESIGN

For the purpose of this research study, the author had chosen to proceed and utilize a quantitative research method to gather the data required, which gave way to analyse the questions posed. This led to further analysis of the results that were then investigated to demonstrate if there are any important indicators that will answer the research question above in section 2.1 and accordingly evaluate the questions raised relating to GDPR awareness.

Quantitative research methods will provide researchers with data that can be ranked or measured to establish general laws of behaviour, which can then be further detailed with the use of graphs or tables as indicators to the readers (McLeod, 2019). The author considered the use of qualitative research methods but ruled this out based on the need for hard facts and data to construct the results in a correct manner. The use of qualitative research methods would not be conducive with this study as hard facts are required as to the awareness of GDPR and the other questions that have been analysed. This may not be quite clear if, as suggested, the interview results from qualitative

methods being used to explore the views, beliefs and experiences of the participants are being attempted to analyse (Gill et al, 2008).

Saunders *'Research Onion'* 2007 [*Figure 1 below*] lays out the process that the author followed through the methods of gathering the data required to make a interpreted informative hypothesis (Huddersfield University, 2019).

The items marked in red within the 'Onion' indicate the actual process that was followed by the author, that being a cross-sectional selection of industry choices to include specific information requested within the online survey, a mono-method of gathering the data, using an online survey only, followed by deductive approach to analyse the responses and finally an interpretive look at the results to finalise the discussion and finally onto the section of conclusions.

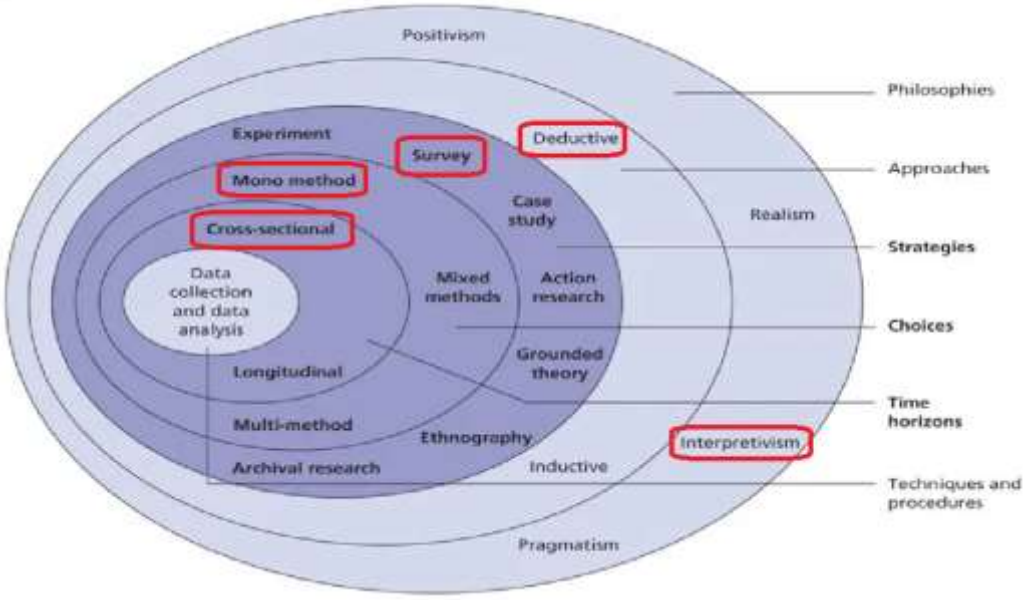


Figure 1: The Research Onion (Saunders et al, 2007)

Quantitative data can be recorded and hence interpreted with statistical analysis, therefore as statistics are based on the principles of mathematics, the quantitative approach is viewed as objective and rational (McLeod, 2019).

3.3 QUESTION DESIGN

The author used a quantitative research design to gather primary data and has been distributed to chosen participants via an online survey method, that being Google Forms.

The questions have been designed using a cross-sectional research method to give simple responses to multiple questions that can be collated in such a way to give indicators against the research question being investigated, namely around GDPR awareness.

The questions were designed to indicate responses regarding industry and GDPR specific queries across a variety of organisations to investigate any similarities or indicators from this perspective only. There is no causation required as this will be discussed in the results and conclusion sections below.

The results were not dependent or require information regarding the individual participants personal details such as, sex, age, location or education etc.…

When choosing a cross sectional research design, the study should be representative of the population as generalizations from the findings will need to be made and have validity (Health Knowledge, 2019). Which was achieved by inclusion of a wide variety of industry sectors which gave limited indicators against the research being investigated.

The survey questionnaire (Appendix 2) was designed to give the best quality indicators that would allow a proper interpretation of the results which would highlight the questions being asked in relation to the awareness of GDPR. There were twenty-six questions in total, which were further broken down into the sub-sections that can relate to each other for the results. Starting questions within the survey were designed to prove the person(s) participating were the correct individuals in the relevant organisation that had responsibility for data protection, GDPR and all relating to, but not necessarily limited to, hardcopy documentation only. This method of questioning provided validation for the scale of results being received and then further analysed, more fundamentally validation that the participants could respond regarding hardcopy documentation within their organisation.

The survey was issued with twenty-six questions *or indicators [Appendix 2.0]* that would give responses for further investigation into the main question of the research. The questions were further broken into various subsections and analysed by the headings below, that will provide the indicative results to the research questions being asked.

Subscale Heading	Quantity of Related Questions
Industry	1
Organisation Size	1
Hardcopy Documents	10
Retention Policies	4
GDPR	10

Based on the research being investigated, the focus was on responses to the survey that are directly related to the actual dissertation title, that being the following 4 main themes for further analysis (in no particular order):

1. GDPR AWARENESS OF THE PARTICIPANT
2. THE INDUSTRY THE PARTICIPANT IS INVOLVED OR EMPLOYED WITHIN
3. WHAT TYPE OF GDPR TRAINING WAS GIVEN TO THE PARTICIPANT
4. FINANCIAL INVESTMENT REQUIRED FOR FURTHER TRAINING

The questions were designed and placed into the distinct groupings above for the following reasons.

1. The main investigation and research questions were based on an individual's awareness of the 2018 GDPR regulations and had a scale of answers to choose from being 'extremely familiar' of the regulations through 4 other options ending in 'not familiar at all'.
2. Next there were very distinct questions on the survey designed around the industry the participant was working in. This led to the ability to analyse the

feedback regarding the GDPR awareness levels within the industry sectors noted.

3. Furthermore, questions were asked specifically relating to the type or quality of training given to the individuals in terms of GDPR compliance, which included a choice of responses from no training given to a great deal of training. Next the questions were based on whether the training was internal, external, formal or informal which would indicate the investment into training on this subject matter by the organisation type.
4. The survey also included important questions relating to whether financial investment in training would be required to obtain and retain GDPR compliance within the respondents organisation and the monetary level of investment required in their opinion.

Other questions and sub-sections contained information requests about the type, quantity and compliance of hardcopy documentation that the organisation has in place which were placed in the survey as confirmation that the participants did in fact have hardcopy documents within their organisations which specifically relates to the subject matter being investigated. Any participant that did not confirm this important section of the survey would be excluded from any further analysis and subsequent results. Further sub-sections pertaining to data breaches and data commissioner fines were also used as indicators to further compound the results that the individuals understood the terminology and the potential impact data breaches may have on their respective organisations. Again, these sub-sections were for indicative purposes only as proof of compliance to the survey subject matter and not being further analysed by the researcher.

3.4 PILOT STUDY

A pilot study was carried out with five participants from the authors direct company contacts and colleagues. The author requested permission directly from the individuals verbally to send them the online survey via email. Full disclosure was given from the beginning of the survey to all participants within

the introduction email asking them to agree to proceed, informing them they could opt-out at any stage by simply closing down the survey and as to the reason behind the questionnaire plus how the results will be calculated and analysed.

The pilot study requested the test participants to provide any additional information feedback on the clarity of the questions based on the theme of the research regarding GDPR awareness and also to the time taken to complete the survey to see if it was overly time consuming to complete, which would have been a negative aspect in order to achieve as much survey completion as possible by the main survey when distributed. The participants were also asked to give feedback on the quality of the questions asked, the ease of understanding what is asked, and finally, whether the participants have any additional constructive criticisms or advice on questions that should or should not be asked. The feedback received was verbal directly between the participant and the author in all five cases. Any feedback was noted locally by the author with any relevant changes made to the online survey set up at the time of receipt.

Some constructive criticism was received back, with thanks, regarding the structure, the focusing of questions and also the setup of the form itself, however the main content questions were received well and well understood in terms of what was being asked of the participants. Some feedback allowed the author to make changes around clarification on responses being extended past the initial YES / NO answers available and the ability to add a free text field in some cases or questions. Some questions were expanded to a scale of responses, but the author avoided any free-text field inclusion so as not to steer away from specific primary data responses for analysis.

3.5 MAIN STUDY

The author has been involved directly within the records management industry over the last 27 years, which gave some in-depth information and relevant detail into the persons who could be chosen to participate in the research study that would consist of professionals within the document management role in their

organisation or data protection officers, business owners or office managers, which are mainly any person who is deemed as the responsible person relating to hardcopy documentation and the relevant GDPR related activities.

The author has chosen to approach potential participants from a variety of industries and company sizes that will be asked to voluntarily respond and participate in the survey and answer the questionnaire issued which will be of a quantitative nature.

The survey questionnaires were issued to participants from a varied cross-section of industry types, organisation size and sectors which would attempt to give a clear picture whether there is any indication that certain size, type or sectoral organisations have understood, provide training to their authorized GDPR person and are dealing with their obligations in the correct manner. The invitees were identified by the author through personal professional knowledge as the person that is responsible for the management of the organisations hardcopy records and documentation that contain confidential data of any kind that could lead to GDPR issues or data breaches at any stage. The survey distributed clarified with the potential participants that the questionnaire was from the author directly, the purpose of the survey and that the responses would be fully confidential which would have been the main concern of the participants at time of receipt. The questionnaires were issued to these participants using online survey methods, namely Google Forms.

The information being gathered was designed to address the main topic related specific questions regarding GDPR awareness & training around GDPR regulations, plus the industry that the person is operating within. Using the Likert Scale of analysis in some pertinent questions, the responses to the questions asked may indicate if there is a link to the organisation sector and awareness in which they are operating within. The Likert Scale assumes that the strength or intensity of an attitude is linear and therefore assumes that the attitude can be measured if the participant is allowed a scale of choices from strongly agree, to strongly disagree (McLeod, 2019). Some questions were retained as YES or NO answers only, which kept any assumption or deflection out of the results as they are clear questions with clear responses required. A

quantitative research approach has been used as it uses logic to deduce criteria and results in which researchers can begin with an research question and collect the data that can be used to determine if there is evidence to support that the hypothesis exists (Statistics Solutions , 2019).

3.6 SAMPLE SIZE

Sample size is very important to give the researcher as many indicators possible to be able to demonstrate any strong response indicators between the themes questioned and put forward in the research. For the purpose of this research investigation the author used a convenience sampling technique as the contacts that were relevant to the study were known professionally at the time of creation. It would be ideal to be in a position to choose an entire population covering all major industries, sectors and businesses, but this is almost impossible to do in any form of research, therefore the researcher must choose and work with a sample size (Gogtay, 2010). The larger the sample size gives a larger results base and gives the researcher as much information as possible to analyse the results, however, these results are seen as indicators to the questions asked based on the participants knowledge or experience and must remain as given with noted limitations.

The survey was sent directly to 110 contacts for participation via email and included as many participants as possible from within the varied industries available to the author.

It was deemed that this sample size was sufficient as it broached on a wide variety of industries and company sizes, including professional data protection officers and managers alike. The survey yielded 95 full responses which gave a resulting amount of non-response bias of 13.6% and a positive response bias of 86.4% of the sample size (Fincham, 2008). Dependent on the type of research being conducted and the industry or reason for the research, a return response rate of > 80% would be deemed a successful return rate to proceed with the analysis in an educational setting, with most researchers in various other industries aiming at a positive response rate of 60% or higher (Fincham, 2008). In normal customer based surveys (non-educational), it is believed that a

response rate to any survey of 50% or more should be deemed as successful, which is very much dependent on a multitude of factors, such as demographic, relationship to researcher, incentive, method and so on (Willott, 2019).

The target participants were chosen based on their industry, knowledge, role within an organisation and company size which would give a clear level of results to analyse and present the findings based on the results highlighting any indicated correlation between the main topics noted.

3.7 ETHICAL CONSIDERATIONS

The research was conducted using online survey methods, adhering to the advised process that all information was disclosed at the outset to ascertain full and clear informed consent to all asked to participate (Shahnazarian et al, 2019). All participants in the full study were given full disclosure to the reasoning behind the study and what information was being asked. The introduction clearly stated that all information is to be submitted to the National College of Ireland and retained for 5 years as per the college's data retention policy. No data was retained that could match any participant with the response received at any stage as to the information being gathered including their respective industry, industry size or the participants personal awareness related to GDPR. The participants were asked to agree to take part and that they understood the information being provided before beginning the actual survey, from that moment on all participants could choose not to participate at all, not to proceed past the opening introduction and then can choose to leave the survey at any time during the questioning. *See Appendix 7 below* (Reeves, 2020)

The author does not believe that there are any ethical concerns or issues that may arise from the questionnaire content.

3.8 CONCLUSION

In Summary, the methodology utilized in the survey were tested and adapted in line with a focused pilot study group, which then confirmed the ability to proceed with the full survey of all participants in the main study. The introductory questions were posed to ascertain the confirmation that the participants could give qualified answers relating to Irish organisations and more importantly relating to hardcopy documentation containing personal data. There were no ethical issues to be concerned with, so the survey was proceeded as planned, which will lead into the results analysis and final discussion and concluding points.

CHAPTER 4 – FINDINGS AND ANALYSIS

4.1 INTRODUCTION

As noted previously, the participants were asked to agree to participate in the survey via an online survey method and were distributed during the month of April and May 2020. All results were received back in a timely fashion for further analysis. Ninety-five surveys were completed and results were returned from the survey request which is an excellent response return rate as noted above (Fincham, 2008), and therefore it was deemed ok to proceed with the analysis.

The findings and analysis below are in the order noted in the above sections, that being:

1. GDPR awareness
2. Industry of the Participant
3. GDPR training received

4.2 GDPR AWARENESS

In this first and most salient section relating to overall GDPR awareness, the analysis of the research results set out to determine if the individual participants to the survey believe what level of awareness and understanding of the GDPR regulations, in their own opinion.

The survey results below are shown in the following order:

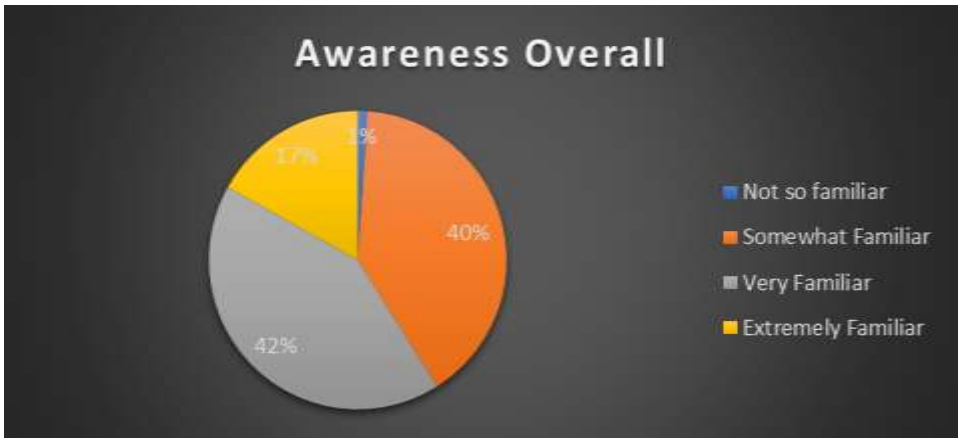
1. Overall awareness *Fig 2.1*
2. Somewhat Familiar with GDPR regulations *Fig 2.2*
3. Very Familiar with GDPR regulations *Fig 2.3*
4. Extremely Familiar with GDPR regulations *Fig 2.4*

To convert the details submitted by participants from the Likert Scale options offered, the choices were converted to a numbering system using numbers 1 to 5, using the Table 2 (pg. 69) template in the appendices below.

The results are as follows and illustrated below in *Fig 2.1:*

- All participants proclaimed some level of awareness of GDPR regulations with varying levels of awareness given, which would be expected based on the target audience, that being professionals that are either directly employed to ensure good GDPR compliance or company owners that have direct responsibility to ensure compliance.
- Zero (0) participants answered that they had 'no knowledge' or awareness of GDPR
- 1 participant or less than 1% of the respondents indicated they are 'Not so Familiar' with the regulations
- 38 participants or 40% of the respondents said they were 'somewhat familiar' with the regulations
- 40 participants or 42% of the respondents indicated they were 'very familiar' with the regulations
- 16 participants or 17% of the respondents are 'extremely familiar' with the GDPR regulations

Fig 2.1



The results to the main driving question as to the awareness of the participants to GDPR regulations would tend to indicate that there is a varying degree of awareness of GDPR for all respondents. However, due to the roles, duties or

status of the targeted participants to the survey, that being managers, professional records managers, business owners and data protection officers the indication that only 16 x participants (or 17%) are extremely familiar with what is required to obtain and retain GDPR compliance even though there should be an innate responsibility on them with risk to the business regarding data breaches being very high to every organisation. In addition, 40 x respondents relating to 42% responded indicating they are very familiar with the GDPR regulations. Only 1 participant which equates to less than 1% responded and agreed they were 'not so familiar' with GDPR regulations who was operating within the 'Services / Manufacturing' industry. The respondent confirmed that they received minimal internal training on GDPR only.

The initial category that was reviewed were the respondents that submitted they were 'somewhat familiar' with the regulations. The total that responded from the overall sample included was 38 participants who submitted this optional result, see Fig 2.3 below.

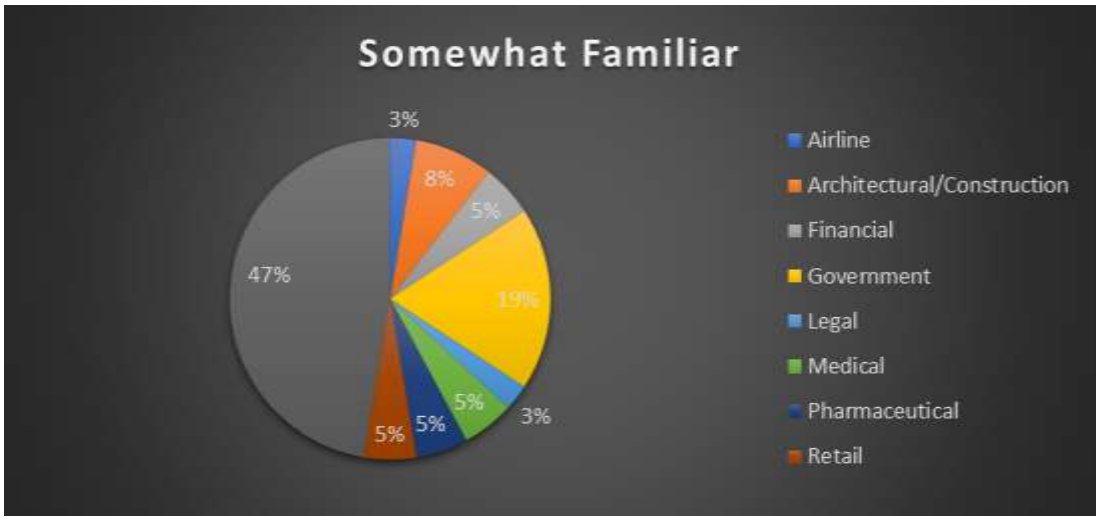
This accounted for 40% of the submissions received. For information purposes only, from the entire sample of results received 47% of the overall respondents were from the 'Services / Manufacturing' industry within this category, see *[Fig 2.2]* below.

Fig 2.2

Industry	Number of Respondents
Airline	1
Architectural/Construction	3
Financial	2
Government	7
Legal	1
Medical	2
Pharmaceutical	2
Retail	2
Services / Manufacturing	18

From the results below, sixteen (16) of the respondents also stated that there would be a financial investment required to get compliant with GDPR regulations, which we will analyse and categorize in sub-section 4.5 below.

Fig 2.3



.

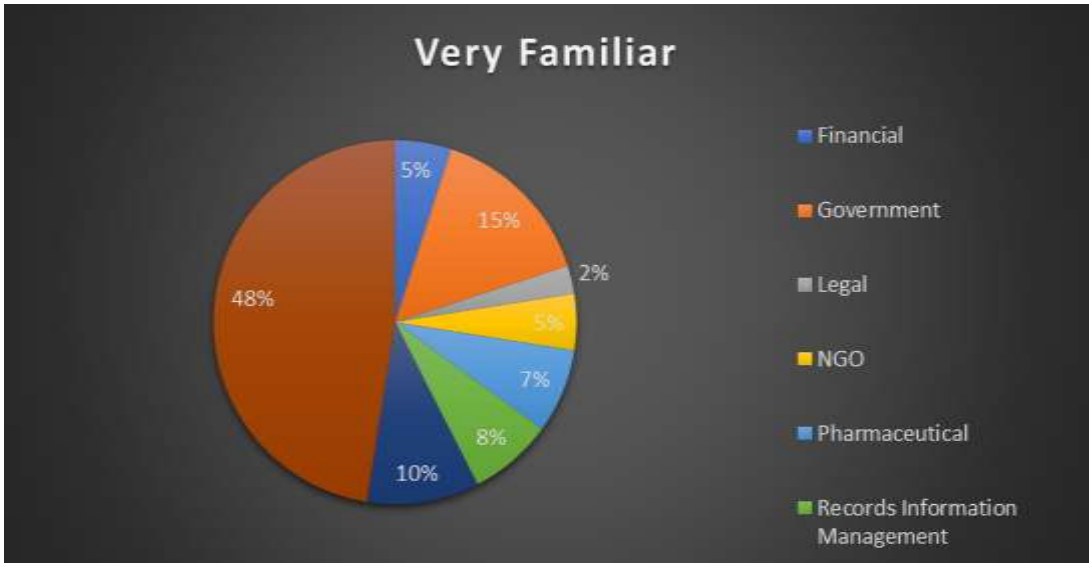
The highest number of participants in the survey categorized themselves in the 'Very Familiar' bracket with regards to GDPR Awareness. Forty respondents that accounted for 42% of the overall results that stated they were within this section of GDPR awareness see *Fig 2.5* below for breakdown per industry sector.

For information purposes only, the industry statistics below in *Fig 2.4* show that the highest number of participants were from the 'Services / Manufacturing' industry at 48% or 19 respondents within this category.

Fig 2.4

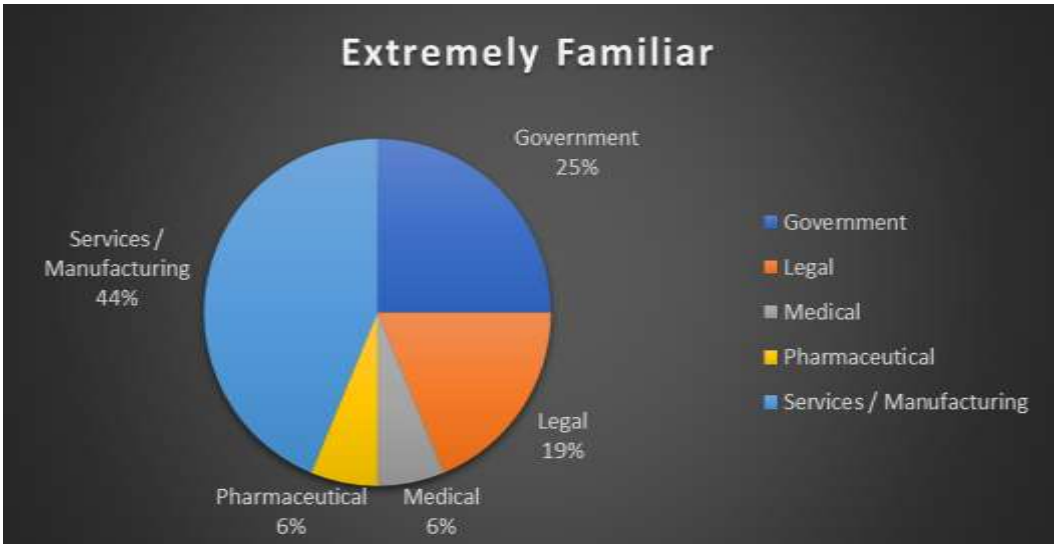
Industry	Number of Respondents
Financial	2
Government	6
Legal	1
NGO	2
Pharmaceutical	3
Records Information Management	3
Retail	4
Services / Manufacturing	19

Fig 2.5



The final category we will review and analyse is the respondents who believe they are 'Extremely Aware' of their GDPR compliance regulations and associated processes and procedures to achieve and remain compliant to GDPR regulations. Out of the total 95 respondents 16 respondents or 17% of these believe they are extremely aware of GDPR regulations, see *Fig 2.6* below.

Fig 2.6



Once again, as per *Fig 2.7* below, the highest proportion of respondents within this section were from the Services / Manufacturing industry at 7 respondents or 44% of the sample received.

Fig 2.7

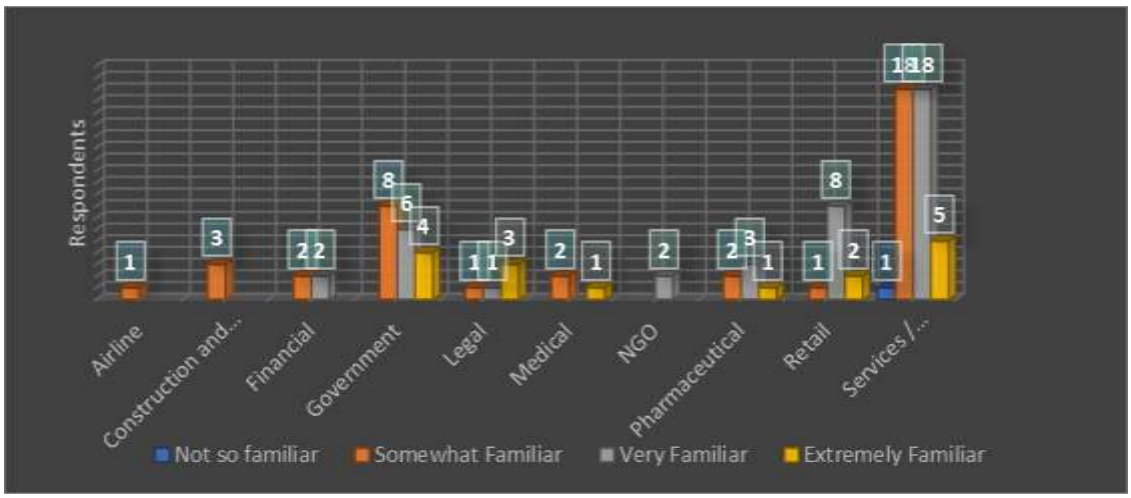
Industry	Number of Respondents
Government	4
Legal	3
Medical	1
Pharmaceutical	1
Services / Manufacturing	7

4.3 INDUSTRY ANALYSIS

To investigate if there is any inference to the above GDPR awareness results against the industry type, we must look closer into the analysis of the industries that the overall total respondents are operating within. The online survey was distributed to a variety of industry practitioners, busines owners and professionals to get a broad sample of primary results which could be further analysed to see if there is a correlation between GDPR awareness and Industry type. In total, there were ten different industries which were included, as shown below in *Fig 2.8.*

In the discussion section (p.50) we will discuss the results findings below in *Fig 2.8* below which could indicate a lower than expected awareness rate in sectors that would tend to handle more personally confidential information and therefore the question could be asked in further research as to why are the results not showing higher awareness rates by the respondents. In particular the awareness levels of respondents in the medical and financial industries where highly confidential personal data is retained, and as shown above in the literature review above, any data breaches can be highly publicized and damaging to the organisations reputation that may be avoided with more rigorous training investments.

Fig 2.8



4.4 GDPR TRAINING PROVIDED BY SECTOR

"Intellectual growth should begin at birth and only cease at death" Albert Einstein

Firstly, we will look at the provision of internal training methods within the organisation with the most obvious benefit of providing internal training is that it is certainly the most cost-effective solution and it is also delivered by other team members that are known to each other which can provide a more relaxed and comfortable atmosphere during the training sessions.

Below in *Fig 2.9* & *Fig 3.0* the results show the total respondents per training type and the percentage % indication of the type of training of GDPR regulations received by the participants to the survey from their respective organisations.

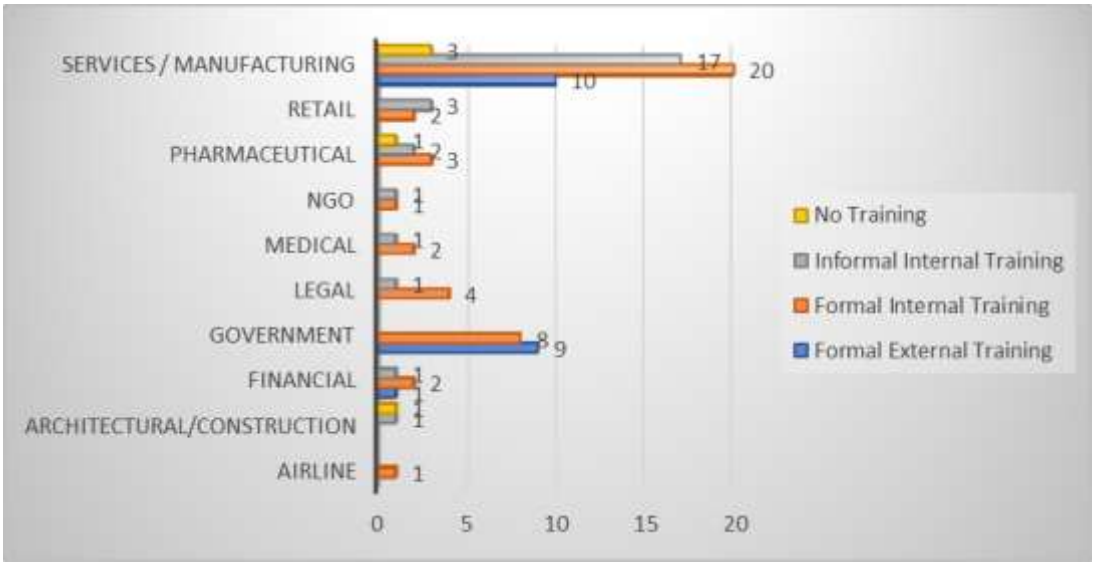
Fig 2.9

Training Received	Total
Formal External Training	20
Formal Internal Training	43
Informal Internal Training	27
No Training	5

Fig 3.0

The analysis shown in *Fig 3.1* below of the results shows the training received by the participants to the survey which would indicate a higher percentage of formal internal training has been given by their respective organisations with the resulting 45% stating this. The next level of training received by individuals is at the what is deemed as informal internal training, resulting in 29% of companies providing this level of GDPR training. Only twenty participants out of ninety-five have received any formal external training regarding GDPR awareness which is only 21% of the participants. Unfortunately, only 5 respondents have stated they received no training whatsoever from their respective organisations which is 5% of the survey total, which should be a cause for concern for said organisations.

Fig 3.1



In conjunction with the above analysis, in *Fig 3.1* above, we will also look at which sectors or industries have shown any trends towards the type of training being provided. As stated above, the main respondents were from the Services / Manufacturing industry with a positive response rate of 53% of the overall survey therefore would be expected to give higher results in all areas.

One of the initial stand out indicators in the above chart *Fig 3.1* is the result for 'Formal External Training' which is mainly divided between the services / manufacturing and government sectors which equate to 19 respondents out of

the twenty who confirmed they received external training, leaving only 1 other respondent that received external training, which came from the financial sector.

Following on from this, the next stages are the formal internal training offerings received by participants, which are also heavily weighted towards the same sectors. In fact, the participants to the survey confirmed that out of the 17 respondents to the survey, only formal training was given either internally or externally.

The remaining industries had a varied response rate which is split between informal and formal internal training only. And notably only 1 respondent had received no training at all from their employer or organisation.

4.5 FINANCIAL INVESTMENT

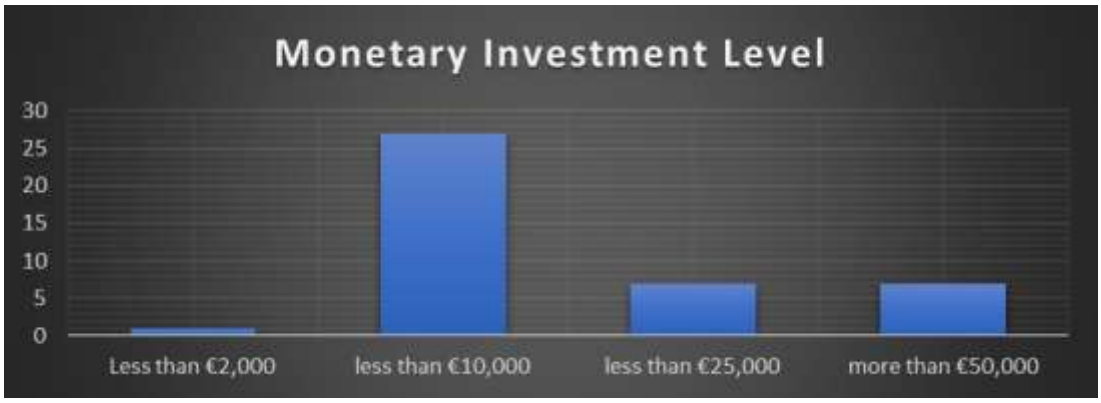
All organisations should always be looking to improve their team's skillsets and capacity levels, which will in turn improve their overall value to the company. As mentioned above, GDPR awareness & training is a key factor to reducing human error issues which any organisation can fall victim to. The type of training is key to the understanding and awareness taken by the employee to their daily roles, so careful consideration must be taken as to whether the training provided will be from an internal or external source, but choosing either should be provided with the highest quality whenever possible. Of course, one of the main considerations is the financial resources required to provide external training sessions (Ranja, 2018).

The results of the survey are shown in *Fig 3.2* below, which would indicate what level of financial investments the respondents believe will be required to be compliant to GDPR regulations and to remain that way with respect to all of their hardcopy documentation.

Of the 95 respondents in total, 46 participants (52%) have stated that they believe that there is some level of financial investment required, with 49 (48%) believing that there is no further investment required to retain or achieve continual GDPR compliance. The vast majority of the respondents, twenty seven or 55% to be exact, believe that the level of investment required would be

less than €10,000, and seven (14%) of the respondents indicating that they believe an investment of over €50,000 would be required for GDPR compliance purposes.

Fig 3.2



CHAPTER 5 – DISCUSSION

The aim of the research was to investigate the level of awareness with regards to the General Data Protection Regulations (GDPR) which was implemented in May 2018. More specifically, the research was aimed towards the person(s) responsible for data protection specifically with hardcopy paper documentation, in Irish organisations.

The importance of compliance is generally known and appreciated throughout the business environment, general public and data process controllers within these organisations (Bauer, 2019).

However, the actual understanding of the regulations in detail would seem to be lacking in some cases where the expectation and rigorous understanding of the regulations should be in place, for example, it was reported that the Irish Justice Department had 41 reported data breaches of sensitive information alone in 2018 (McDonagh, 2019), where one would expect a high level of awareness, training, competency and security with regards to the information that they would process and retain.

This is also noted in the results returned to the authors survey which showed 78% of respondents admitting that they were not extremely aware of the GDPR regulations. While this may seem acceptable to some extent, in order to alleviate the potential for future data breaches, organisations should look to advance everyone in this area of responsibility to being extremely familiar with GDPR regulations. Similarly, there have been multiple reported incidents of data breaches of medical records from hospitals, with some ending up on rubbish dumps, left on busses, left in pubs and other publicly accessed areas. In fact, the HSE reported 465 data breaches in 2019 alone (McDonagh, 2019), where again it may be clearly expected that highly sensitive material of this content would be subject to higher scrutinization and control. Based on the results of the industry analysis of respondents, 33% claimed to be extremely familiar with GDPR, but 66% responded saying they were somewhat familiar, or less, with GDPR regulations which could be a cause for concern for regulators within the medical / hospital sector. There are variety of articles published that note that hospital records have been found in very unusual areas &

circumstances, as noted above, the HSE reported 465 data breaches in 2019, which is unacceptable in any circumstances much less items of documentation that contain a patients very sensitive information being found in very public areas (Shiel, 2018).

The areas the author would recommend further investigation and analysis are around awareness in detail to specific areas of GDPR, namely awareness of actual retention periods of the information, the handling of the information and the subsequent action to remove and securely destroy the information when it is no longer required to be retained. The basis of this conclusion and recommendation is based on the overall returned results of the authors online survey showing that 78% of respondents were very familiar with the GDPR regulations, with a key part of the GDPR regulations being that personal data / information should only be retained as long as is necessary for the use of the business and only a properly trained person that is extremely aware of the requirements under GDPR would be aware of these requirements and how to deal with them to be compliant. Another example for further research would be that the Data Protection Commissioner recommended hospitals to update their tracking systems considerably to handle the vast amount of medical records retained (Data Protection Commissioner , 2018), an in-depth research may be undertaken to see if this has been followed through also which would mitigate some data breaches recurring again.

The author also researched and detailed what the position is for individuals with regards to their right to privacy in Ireland, which is important as organisations that process or control such information must also be aware of their rights and responsibilities in this regard. The results were subsequently analysed and demonstrated a basic level of awareness for all individuals who responded to the online survey, with only 17% of the respondents declaring that they are extremely familiar with the regulations. The target audience for the survey were professional individuals that either worked directly with hardcopy documentation that contained personal information for individuals to that organisation or they were direct business owners who are also personally responsible for the data being retained by their company. The organisations were chosen across a

broad variety of sectors to show a broader view of the business areas that all record and retain personal data on behalf of individuals.

The low declaration level of highly detailed extreme awareness of GDPR can be perceived as demonstrating a deficit of highly trained and skilled persons within Irish organisations regarding GDPR regulations who could assist to ensure compliance for the organisation they are employed within, were the awareness needs to be at a higher level to protect the organisation and the data alike. On the day of August 15th 2020, one well known employment agency in Ireland was advertising for 67 Data Protection Officer roles in Ireland (Indeed Ireland , 2020), which is indicative with a deficiency in suitable candidates.

The research yielded results showing that a total of 66% of respondents received formal GDPR training and of that only 21% received actual professional external training where, as suggested by Woodman, the quality and focus of external training should be provided whenever possible (Woodman, 2019). 45% of respondents said that they received formal internal training, and it is noted in some cases it is suggested that internal training would be preferable and can identify specific skills for future roles within the organisation (Heathfield, 2020), however, if the current internal practices are not up to compliance standards then passing on of this information internally will not increase the awareness or ability to assist the organisation in the right manner.

The overall awareness of the responsible person within the organisation in knowing, understanding, appreciating and acting to be as compliant to GDPR regulations on an ongoing basis is key to limiting the potential exposure of that organisation to fines, data breach reporting and potential reputational damage. Currently the Data Protection Office does not require all organisations to have a designated Data Protection Officer (DPO), nor does it require a certain level of qualification regarding data protection basing this on the varying types of business in operation (Data Protection Office, 2020).

To increase the levels of understanding and awareness of the GDPR regulations, the author would recommend that it should be considered to put in place the absolute minimum requirement to have at least one professionally qualified and certified Data Protection person within every organisation that

records and retains personal information. There is a requirement under GDPR for certain organisations such as public bodies to elect a Data Protection Officer (DPO), however there is no minimum requirement to have more than one per head of capita in the organisation or any stipulation to ensure that there is a certain level of qualifications in place (Data Protection Commission, 2020). Furthermore, any increase in the business size will have a knock-on effect on the area of compliance within the organisation, and therefore would require certified personnel to be put in place after receiving professional external qualifications. There are many qualifications required within businesses that can be taken online and have a specific level to reach to achieve the qualified status, for example, all organisations are required to have a qualified First Aid person at each location, with the numbers increasing depending on the amount of people in the area (Health and Safety Authority , 2020), therefore, the author would recommend this similar type of legislation to be expanded to cover GDPR, data protection and compliance.

The results of the research detailed with regards to GDPR training received by the respondents would indicate similar findings to the survey conducted by McCann Fitzgerald in November 2018 were businesses surveyed admitted that the costs of GDPR implementation were above expectations at that time. Furthermore, 58% of the participants in the same McCann Fitzgerald survey said that the overall costs to date in relation to GDPR regulatory compliance was between €50,000 and €250,000 which included costs for training, the legal, audit and IT departments (Lavery & McKenna, 2018). This report covered large scale businesses in Ireland which would expect such a high investment, however, the basic training required to understand the companies obligations with regards to GDPR would require an entry level, but highly detailed, understanding of GDPR requirements that should not require such high investment amounts as offered by the Irish Academy of Computer Training (IACT) who offer a basic online course at €25 per person which would give a very basic understanding and awareness of GDPR (IACT, 2019). This requirement would compound the same observation made by NatWest Bank that all staff should have a basic understanding of GDPR with different levels of training being given to other as needed (Natwest Bank , 2020).

The penalties that can be applied to any organisation by the DPC can be substantial of up to €20,000,000 or 4% of the annual turnover (McGuone, 2018), so the readiness and continued compliance to GDPR is extremely important to be in place. Especially as the Data Protection Commissioner expects to see a vast increase in reported breaches and has stated she will have no hesitation in investigating these breaches further (Mayer, 2019).

CHAPTER 6 – CONCLUSION

6.1 CONCLUDING POINTS

The overall aim of the research was to establish the levels of awareness regarding GDPR regulations within Irish organisations, specifically in relation to hardcopy documentation. Due to the relative recent adoption of GDPR regulations within Ireland and the wider European, Union the full understanding, awareness and compliance to GDPR is still relatively unknown. There is a general awareness of the wording of GDPR and data protection, however, the detailed understanding of the requirements and potential risks have been called into question in this study based on the examples of data breaches outlined in the literature review section. The focus of the research was towards hardcopy paper documentation only and specifically within Irish organisations.

To begin with the overall personal awareness of GDPR of the respondents to the online survey was questioned and analysed, which yielded a result of 59% being either very familiar or extremely familiar with the GDPR regulations. The remaining 41% reported they were not so familiar or not at all familiar with the requirements of GDPR. Based on the target audience to the survey being the persons specifically responsible for hardcopy records within their respective organisation, the author would surmise that this level of awareness is not at a level high enough for these individuals specifically as they are the responsible persons or qualified persons whose role it is to comply with GDPR on behalf of their respective organisations.

The industry analysis of the respondents regarding their awareness of GDPR gave resulting information that would also cause interest and may be an opportunity to carry out further research. That being, respondents from the Financial services industry scored 50% somewhat familiar and 50% very familiar with zero respondents being extremely familiar (based on 4 respondents). The medical records specific respondents reported as 66% being very familiar and 33% being extremely familiar (out of 3 respondents), finally one more notable category is from respondents in the Government sector who reported 45% where somewhat familiar, 33% were very familiar and 22% were extremely familiar (out of 18 respondents). The author would have

considered the type of personal data held within these organisations or sectors to be of the most confidential information in many cases and therefore would have expected to see a more reported response towards the individuals being extremely aware of GDPR.

Moving more into the training that was provided to the respondents with regards to GDPR compliance, which returned a result of only 21% receiving professional formal external training, and 45% reporting they received formal internal training in this regard. The remaining 29% of respondents reported they received informal internal training and 5% received no training at all. Based on the research around training the author would recommend that only dedicated professional external training be provided to all responsible persons which would provide concise, detailed and highly accurate training with no opportunity for legacy practices to be passed on through internal training methods. There should be no doubt that any lapse in protocol which leads to a data breach can cause huge potential risks to the organisation, including financial penalties and reputational damage alike. If the responsible person is not trained and aware of this fact to its fullest extent, or is trained in a less than competent manner, then expectations to avoid future data breaches are limited.

Finally, we reviewed the financial investment that the respondents believed that their organisations would need to provide to obtain and retain GDPR compliance, with the results ranging from less than €2,000, to 14% believing that an investment of over €50,000 is required to be compliant with GDPR. The majority of 55% believed that a financial investment of less than €10,000 would be required for this compliance to be of the standard required. As discussed in the above section (Chapter 5: Discussion, pg50), there are online entry level GDPR awareness courses within Ireland starting at €25, which also range to the higher level of classroom courses over multiple days to receive a qualification of Data Protection Practitioner Certificate costing approximately €595 per person. The author believes that this level of investment per person is more than required and justified to increase the level of awareness of the individual which in turn provides additional protection to the business as a whole when it relates to GDPR regulations.

The Data Protection Commission now has increased powers to admonish any organisation who does not comply with GDPR regulations and hence suffers a data breach because of this, therefore it is incumbent on the organisation to ensure that their business is protected as best they can regarding GDPR. The DPC have reported annual increases in data breach complaints from the public who are more aware of their own rights regarding their information, therefore the author believes it should be taken extremely seriously that each business needs to provide the investment in their systems, people and processes to protect the sensitive hardcopy information it retains and processes for their businesses requirements.

6.2 RECOMMENDATIONS FOR FURTHER RESEARCH

The author could recommend the following areas for further research, firstly, into what will it take to be in a position that the same participants to this survey would deem themselves as 'extremely familiar' to GDPR awareness and what, if anything, has not been given or can be given to take them to the next level of understanding and awareness. A more detailed investigation into what training can now be provided to increase the awareness levels of all persons to a higher level which will in turn provide increased protection to the organisation.

As noted in the discussion section of the paper, the data protection commissioner advised the hospital sector that they should improve their tracking systems from manual tracking in most cases to an electronic system to alleviate some potential for further data breaches. Further investigation into whether this has been specifically carried out across the hospital sector could be warranted which would demonstrate the willingness to invest in this area.

Hardcopy paper documentation is in abundance in many organisations and has been for some time. Whether the records are retained and stored internally or with a third-party provider is irrelevant in the case of what retention periods have been implemented and carried out. What has been done to become compliant in relation to items held pre-May 2018 when the new GDPR regulations have been completed. Further investigation by industry sector

could be undertaken that will demonstrate the level of investment required to become compliant in relation to these legacy records.

Retention periods differ throughout various industries and organisations with similar minimum periods of retention being advised in some cases only, however, should there not be a clear and concise legislative requirement on minimum retention periods for certain types of documents containing personal data or information?

Training requirements for all organisations has been discussed above by the author, further investigation into organisations as to why they do not offer or insist on a minimal standard of qualification for all people who handle sensitive information of any kind could be considered. Furthermore, what level of training would they require for their specific organisation to increase awareness levels so that all responsible personnel are extremely comfortable and familiar with the organizational requirements to be compliant.

There were differences noted in the quantity of reported GDPR data breach notifications between Ireland and Italy in 2019 (Gorey, 2020). The investigation into any cultural differences that caused differences in official breach reporting could be further researched.

6.3 LIMITATIONS

In the generation of this research dissertation there were some limitations experienced throughout, for example, in relation to the intended target audience of the survey where the author attempted to make contact with a wide variety of individuals from as broad a spectrum of main industry sectors in Ireland. 110 requests to participate were sent to individuals, with a positive response rate of 95 participants completing the survey, giving a positive return rate of over 86%. However, the spread of the industries was reduced because of the non-participation of some individuals, leading to a much higher respondent rate from professionals within the services & manufacturing industry leading to a response rate of 44% of the overall participant group being from the services & manufacturing industries. The next highest being from the ‘Government’ sector

at 19%, with the remaining sectors noted making up the final 37%. For a more detailed and balanced research investigation a set number of data protection professionals in a balanced amount or organisations per industry could be considered.

Due to the virtual newness of the implementation of the GDPR regulations in May 2018, there have been no research investigations completed regarding GDPR regulations within Irish companies and more specifically in relation to hardcopy documentation. This lack of previous research limited the authors ability to have accredited reference material and similar survey templates for similar academic works.

Further limitations to this study were around the pandemic of COVID-19 causing the country to go into lockdown during the timeframes which the survey was intended to be responded to by all. Some further potential participants were either not working, not accessible as they were working from home or not available at their normal contact address, therefore the sample size was not as large as would have been in other normal circumstances.

The researcher is employed directly within the records management industry and had to be extremely careful not to allow any personal bias to dictate the research survey questions or steer the responses and analysis.

REFERENCES

Afifi-Sabet, K., 2018. *People are more aware of their data rights than ever before, says ICO.* [Online]
Available at: https://www.itpro.co.uk/information-commissioner/31565/people-are-more-aware-of-their-data-rights-than-ever-before-says-ico
[Accessed 28th May 2020].

Association of Data Protection Officers, 2020. *GDPR Training Essentials.* [Online]
Available at: https://www.dpo.ie/training/gdprtrainingessentialsclassroom
[Accessed 13th May 2020].

Bauer, J., 2019. *www.nowsecure.com.* [Online]
Available at: https://www.nowsecure.com/blog/2019/03/20/how-the-gdpr-raises-public-awareness-about-privacy/
[Accessed 9th December 2019].

Bolger, P., 2018. GDPR and employee data. *Accountancy Ireland* , February , pp. 43 - 45.

Brennan, D., 2018. *A&L Goodbody: Irish Governemnt publiches Data Protection Bill 2018.* [Online]
Available at: https://www.irelandip.com/2018/02/articles/cyber-risk-data-privacy/irish-government-publishes-data-protection-bill-2018/
[Accessed 6th May 2020].

Brodies Law Firm, 2018. *Business Survey on GDPR,* Edinburgh: Brodies.

Cakebread, C., 2019. *You're not alone, no one reads terms of service agreements.* [Online]
Available at: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T
[Accessed 28th May 2020].

Citizens Information , 2018. *Fundamental rights under the Irish Constitution.* [Online]
Available at:
https://www.citizensinformation.ie/en/government_in_ireland/irish_constitution_1/constitution_fundamental_rights.html
[Accessed 6th May 2020].

Citizens Information , 2019. *Fundamental rights under the Irish Constitution.* [Online]
Available at:
https://www.citizensinformation.ie/en/government_in_ireland/irish_constitution_1/constitution_fundamental_rights.html
[Accessed 25th May 2020].

Craig, W., 2010. *www.WEBFX.com.* [Online]
Available at: https://www.webfx.com/blog/web-design/the-history-of-the-internet-in-a-nutshell/
[Accessed 27th April 2020].

Data Conversion, 2019. *GDPR Data Breaches.* [Online]
Available at: https://dataconversion.ie/gdpr-databreaches/
[Accessed 11th May 2020].

Data Protection Commission , 2020. *Pre-GDPR.* [Online]
Available at: https://www.dataprotection.ie/en/pre-gdpr
[Accessed 6th May 2020].

Data Protection Commission , 2019. *2019 Annual Report.* [Online]
Available at: https://www.dataprotection.ie/en/data-protection-commission-publishes-2019-annual-report
[Accessed 28th May 2020].

Data Protection Commission , 2020. *Data Protection and the General Data Protection Regulation (GDPR).* [Online]
Available at: https://dbei.gov.ie/en/Data-Protection/#:~:text=It%20came%20into%20force%20across,Protection%20Acts%201988%2D2018).
[Accessed 22nd July 2020].

Data Protection Commission, 2018. *Annual Report ,* Ireland : Data Protection Commission .

Data Protection Commission, 2020. *Guidance on appropriate qualifications for a Data Protection Officer (GDPR).* [Online]
Available at: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officrs/guidance-appropriate-qualifications
[Accessed 12th August 2020].

Data Protection Commissioner , 2018. *Data Protection Investigation in the Hospitals Sector,* Dublin, Ireland : Data Protection Commissioner.

Data Protection Office, 2018. *What is the difference between the DPA 2018 and the GDPR? (and why does it matter?).* [Online]
Available at: https://www.dpocentre.com/difference-dpa-2018-and-gdpr/
[Accessed 25th May 2020].

Data Protection Office, 2020. *Guidance on appropriate qualifications for a Data Protection Officer (GDPR).* [Online]
Available at: https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-officrs/guidance-appropriate-qualifications
[Accessed 9th August 2020].

Deloitte LLP, 2018. *A New Era for Privacy - GDPR six months on,* United Kingdom: Deloitte LLP.

Doyle, E., 2019. *One Year Later, is GDPR working?.* [Online]
Available at: https://www.philiplee.ie/one-year-later-is-gdpr-working/
[Accessed 11th December 2019].

DPC, 2019. *Annual Report 2018,* Dublin, Ireland: Data Protection Comission.

DPC, 2019. *Data Protection Commission.* [Online]
Available at: https://www.dataprotection.ie/en/individuals/know-your-rights/right-access-information
[Accessed 10th December 2019].

DPC, 2019. *Data Protection Commission.* [Online]
Available at: https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification
[Accessed 11th May 2020].

Dunne, B., 2018. *GDPR Data Retention.* [Online]
Available at: https://www.siliconrepublic.com/enterprise/gdpr-data-retention

European Data Protection Board, 2019. *First Significant Fine Was Imposed for the Breaches of the General Data Protection Regulation in Lithuania.* [Online]
Available at: https://edpb.europa.eu/news/national-news/2019/first-significant-fine-was-imposed-breaches-general-data-protection_en
[Accessed 25th May 2020].

European Parliament Council, 2018. *Eur-Lex Access to the European Law.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504
[Accessed 9th December 2019].

Facility Executive , 2019. *Many Workers Still Prefer Paper Over Digital Media.* [Online]
Available at: https://facilityexecutive.com/2019/05/many-workers-still-prefer-paper-over-digital-media/
[Accessed 20th May 2020].

Fincham, J. E., 2008. *Response Rates and Responsiveness for Surveys, Standards, and the Journal.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2384218/
[Accessed 7th June 2020].

GDPR Associates , 2019. *Why is GDPR so important.* [Online]
Available at: https://www.gdpr.associates/why-is-gdpr-so-important/
[Accessed 1st June 2020].

Gill et al, 2008. *Methods of data collection in qualitative research: interviews and focus groups.* [Online]
Available at: https://www.nature.com/articles/bdj.2008.192
[Accessed 18th May 2020].

Gogtay, N. J., 2010. *Principles of sample size calculation.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2993982/
[Accessed 7th June 2020].

Gorey, C., 2020. *Silicon Republic.* [Online]
Available at: https://www.siliconrepublic.com/enterprise/ireland-data-breaches-gdpr-fines
[Accessed 11th May 2020].

Health and Safety Authority , 2020. *First Aid.* [Online]
Available at:
https://www.hsa.ie/eng/Topics/First_Aid/First_Aid_Frequently_Asked_Questions/First_Aid_FAQ_Responses/
[Accessed 9th August 2020].

Health Knowledge, 2019. *Introduction to study designs - cross-sectional studies.* [Online]
Available at: https://www.healthknowledge.org.uk/e-learning/epidemiology/practitioners/introduction-study-design-css
[Accessed 18th May 2020].

Health Service Executive, 2020. *Human Failure.* [Online]
Available at: https://www.hse.gov.uk/construction/lwit/assets/downloads/human-failure.pdf
[Accessed 1st June 2020].

Heathfield, S., 2020. *Tap the Power of Internal Training.* [Online]
Available at: https://www.thebalancecareers.com/tap-the-power-of-internal-training-1919298
[Accessed 22nd July 2020].

Hospelhorn, S., 2020. *Varonis - Company reputation after a data breach.* [Online]
Available at: https://www.varonis.com/blog/company-reputation-after-a-data-breach/
[Accessed 1st June 2020].

Huddersfield University, 2019. *Empowering Local Governments in Making Cities Resilient To Disasters,* Huddersfield: Huddersfield University.

I.T Governance , 2020. *GDPR Penalties.* [Online]
Available at: https://www.itgovernance.eu/en-ie/dpa-and-gdpr-penalties-ie
[Accessed 20th May 2020].

IACT, 2019. *Employee GDPR Training.* [Online]
Available at: https://iact.ie/gdpr-solutions/employee-gdpr-training/
[Accessed 18th December 2019].

ICS, 2019. *Survey Reveals Record Number of Data Breaches in Irish Companies.* [Online]
Available at: https://www.ics.ie/news/view/842
[Accessed 6th May 2020].

Indeed Ireland , 2020. *Data Protection Officer Jobs.* [Online]
Available at: https://ie.indeed.com/Data-Protection-Officer-jobs
[Accessed 15th August 2020].

International Association of Privacy Professionals (IAPP), 2019. *Get GDPR ready.* [Online]
Available at:
https://iapp.org/train/gdprready/?gclid=Cj0KCQiAuefvBRDXARIsAFEOQ9ES8YkiF5xEJ4TvX1OVZ9vlD3oLPhIxC8JiG-TeZYBG4dSbnIffjyYaAlLhEALw_wcB
[Accessed 18th December 2019].

Irish Computer Society, 2020. *More than half of Irish Companies have suffered a data breach within the past year.* [Online]
Available at: https://www.ics.ie/news/view/1361
[Accessed 20th May 2020].

Irish Statute Book, 2018. *Data Protection Act 2018.* [Online]
Available at: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
[Accessed 6th May 2020].

Kearney, S., 2019. *GDPR: Privacy considerations for the Digital Single Market,* Dublin: Journal of Internet Law.

Lavery & McKenna, 2018. *A Survey of the Impact of GDPR and its effect on Organisations in Ireland,* Dublin, Ireland: McCann Fizgerald & Mazars.

Liu, R., 2019. *The Growth of the Cloud and the Reasons Why.* [Online]
Available at: https://medium.com/swlh/the-growth-of-the-cloud-and-the-reasons-why-865f8fc8525f
[Accessed 20th May 2020].

London Business Training & Consulting, 2020. *Importance of Business Training For an Organisation.* [Online]
Available at: https://www.lbtc.co.uk/business-management-training-blog/importance-of-business-training-for-an-organisation/
[Accessed 22nd July 2020].

Lush, M., 2019. *NSF newsroom: Human Error Prevention; Solutions and Answers.* [Online]
Available at:
https://www.nsf.org/newsroom_pdf/pb_human_error_prevention_solutions_and_answers.pdf
[Accessed 1st June 2020].

Mayer, D., 2019. *Holding a big stick over big tech ,* Dublin, Ireland : Focus Magazine .

McDonagh, D., 2019. *41 Breaches of sensitive data recorded at the Justice Department.* [Online]
Available at: https://www.independent.ie/irish-news/41-breaches-of-sensitive-data-recorded-at-justice-department-38374342.html

McDonagh, D., 2019. *HSE data breaches: Misplaced patient records discovered in pub, lost medical files turned up on bus.* [Online]
Available at: https://www.independent.ie/irish-news/health/hse-data-breaches-misplaced-patient-records-discovered-in-pub-lost-medical-files-turned-up-on-bus-38298556.html
[Accessed 11th May 2020].

McElhill, D., 2019. *Personal Data Breaches - to notify or not to notify.* [Online]
Available at: https://dpnetwork.org.uk/opinion/personal-data-breaches-to-notify-not-to-notify/
[Accessed 25th May 2020].

McGuone, C., 2018. Is Your Practice GDPR ready?. *Vetirinary Ireland ,* 7(12), p. 644.

McKenna & Lavery, 2018. *Irish Businesses taking GDPR Compliance in their Stride,* Dublin, Ireland: MCCann Fitzgerald.

McLeod, S., 2019. *Likert Scale Definition, Examples and Analysis.* [Online]
Available at: https://www.simplypsychology.org/likert-scale.html#:~:text=The%20most%20widely%20used%20is,disagree%20with%20a%20particular%20statement.
[Accessed 7th June 2020].

McLeod, S., 2019. *Simply Psychology.* [Online]
Available at: https://www.simplypsychology.org/qualitative-quantitative.html
[Accessed 25th January 2020].

McLeod, S., 2019. *What's the difference between qualitative and quantitative research?.* [Online]
Available at: https://www.simplypsychology.org/qualitative-quantitative.html
[Accessed 18th May 2020].

Millaken, G., 2014. *WIRED.* [Online]
Available at: https://www.wired.com/insights/2014/01/paperless-office-30-year-old-pipe-dream/
[Accessed 27th April 2020].

Moore, L., 2018. *GDPR with an Irish flavour – The Irish Data Protection Act 2018.* [Online]
Available at: https://inplp.com/latest-news/article/gdpr-with-an-irish-flavour-the-irish-data-protection-act-2018/
[Accessed 25th May 2020].

Nathan Trust , 2020. *GDPR Fines and Penalties.* [Online]
Available at: https://www.nathantrust.com/gdpr-fines-penalties
[Accessed 28th May 2020].

National College of Ireland, 2018. *National College of Ireland.* [Online]
Available at: https://www.ncirl.ie/Portals/0/QA/Handbook/NCIQAH-9.%20Information%20Governance.pdf?ver=2019-07-30-153800-903
[Accessed 25th January 2020].

Natwest Bank , 2020. *Staff training for GDPR.* [Online]
Available at: https://natwestbusinesshub.com/articles/staff-training-for-gdpr
[Accessed 15th June 2020].

O'Halloran, M., 2014. *Constitutional right to privacy has to be considered in adoption tracing Bill - Minister.* [Online]
Available at: https://www.irishtimes.com/news/politics/oireachtas/constitutional-right-to-privacy-has-to-be-considered-in-adoption-tracing-bill-minister-1.1740965
[Accessed 25th May 2020].

Pepper, T., 2020. *CPO Magazine.* [Online]
Available at: https://www.cpomagazine.com/cyber-security/accidental-internal-data-breaches-are-on-the-rise-heres-how-to-protect-your-business/
[Accessed 20th May 2020].

Pinto, S., 2018. *Privacy and data protection : A study on awareness and attitudes of millennial consumers on the internet; an Irish perspective.* Dublin : National College of Ireland (Unpublished Thesis) .

Printing Impressions, 2015. *PRinting Impressions.* [Online]
Available at: https://www.piworld.com/article/reading-paper-reading-screens-u-s-consumers-prefer/
[Accessed 6th May 2020].

Quinn, H., 2016. GDPR and traning your staff. *Veterinary Ireland ,* 8(5), pp. 260-261.

Quinn, H., 2018. GDPR and Training your Staff. *Veterinary Ireland,* 8(5), pp. 260-261.

Ranja, S., 2018. *Inhouse VS External Training: Which One Is Best For You?.* [Online]
Available at: https://www.indepthresearch.org/blog/inhouse-vs-external-training-which-one-is-best-for-you/
[Accessed 17th June 2020].

Reeves, G., 2020. *GDPR Awareness (Thesis,* Dublin : NCI .

Reynolds, S., 2018. A Breach of GDPR – the Consequences. *The Parchment ,* Winter (https://www.kanetuohy.ie/wp-content/uploads/2018/12/Sarah-Reynolds-Parchment_Winter_2018-1.pdf), pp. 22 - 23.

Sarap, K., 2019. *Three reasons why we need strict data protection regulations.* [Online]
Available at: https://www.njordlaw.com/three-reasons-need-strict-data-protection-regulations/
[Accessed 1st June 2020].

Science Direct, 2019 . *Science Direct - Positivism.* [Online]
Available at: https://www.sciencedirect.com/topics/social-sciences/positivism
[Accessed 25th January 2020].

Secretary to the College , 2016. *Records Retention Schedule ,* Dublin, Ireland : Trinity College Dublin .

Shahnazarian et al, 2019. *Office for the Protection of Research Subjects,* Los Angeles: University of Southern California.

Shannon, J., 2018. *New law bans advertisers targeting kids online.* [Online]
Available at: https://irishheart.ie/news/new-law-bans-advertisers-targeting-kids-online/
[Accessed 29th July 2020].

Shiel, T., 2018. *Hospital apologises to patients over medical records found in estate.* [Online]
Available at: https://www.irishtimes.com/news/ireland/irish-news/hospital-apologises-to-patients-over-medical-records-found-in-estate-1.3640980
[Accessed 11th May 2020].

Shiel, T., 2018. *Hospital apologises to patients over medical records found in estate.* [Online]
Available at: https://www.irishtimes.com/news/ireland/irish-news/hospital-apologises-to-patients-over-medical-records-found-in-estate-1.3640980
[Accessed 12th August 2020].

Statistics Solutions , 2019. *Statistics Solutions.* [Online]
Available at: https://www.statisticssolutions.com/quantitative-research-approach/
[Accessed 16th December 2019].

Survey Monkey, 2019. *Survey Monkey.* [Online]
Available at: https://www.surveymonkey.com/mp/likert-scale/
[Accessed 25th January 2020].

Survey Monkey, 2019. *Survey Monkey.* [Online]
Available at: https://www.surveymonkey.co.uk/
[Accessed December 2019].

Tech Central , 2019. *The biggest data breach fines, penalties and settlements to date.* [Online]
Available at: https://www.techcentral.ie/the-biggest-data-breach-fines-penalties-and-settlements-to-date/
[Accessed 6th May 2020].

Technology Committee , 2018. *Retention or Destruciton of Files,* Dublin, Ireland: The Law Society of Ireland .

Termsfeed, 2020. *Examples of "Click to Accept".* [Online]
Available at: https://www.termsfeed.com/blog/examples-click-accept/
[Accessed 28th May 2020].

The Grand Hotel , 2018. *The Grand Hotel - Retention Policy.* [Online]
Available at: https://www.thegrand.ie/files-sbbasic/ba_grand_ie/data-retention-policy-grand-hotel.pdf
[Accessed 11th May 2020].

The Irish Times, 2019. *Google hit with €50m fine for data privacy breach.* [Online]
Available at: https://www.irishtimes.com/business/technology/google-hit-with-50m-fine-for-data-privacy-breach-1.3765575
[Accessed 11th December 2019].

The Law Reform Commission , 1998. *Report on Privacy: Surveillance and the Interception of Communications ,* Dublin: The Law Reform Commission .

Troy, D., 2017. *Internal Vs. External Training: Which Is Right For You?.* [Online]
Available at: https://elearningindustry.com/internal-vs-external-training-right
[Accessed 15th June 2020].

Uzialko, A., 2018. *How Businesses Are Collecting Data (And What They're Doing With It).* [Online]
Available at: https://www.businessnewsdaily.com/10625-businesses-collecting-data.html
[Accessed 28th May 2020].

Willott, L., 2019. *Average Survey Response Rate – What You Need to Know.* [Online]
Available at: https://www.customerthermometer.com/customer-surveys/average-survey-response-rate/#:~:text=A%20survey%20response%20rate%20of,range%20are%20far%20more%20typical.
[Accessed 7th June 2020].

Woodman, C., 2019. *The Advantages of Outside Trainers for Employees.* [Online]
Available at: https://smallbusiness.chron.com/advantages-outside-trainers-employees-21939.html
[Accessed 22nd July 2020].

www.cro.ie, 2019. *Companies REgistration Office.* [Online]
Available at: https://www.cro.ie/Publications/Company-Forms
[Accessed 10th December 2019].

www.gov.ie, 2020. *Data Protection and the General Data Protection Regulation (GDPR).* [Online]
Available at: https://www.gov.ie/en/organisation-information/26c38c-data-protection-and-the-general-data-protection-regulation-gdpr/
[Accessed 27th April 2020].

www.iccl.ie, 2019. *Her Right to Privacy.* [Online]
Available at: https://www.iccl.ie/her-rights/privacy/
[Accessed 27th April 2020].

APPENDICES

Appendix 1

CRO business registration form

CRO - RBN1A v2 fillable.pdf

Appendix 2

Online Questionnaire

GDPR Awareness and Associated Training -

Appendix 3

The Law Society of Ireland

The LSI - retention[1].pdf

Appendix 4

Trinity College Dublin

TCD - Records Management Policy.p

Appendix 5

National College of Ireland

NCIQAH-9. Information Governa

Appendix 6

Health Service Executive (HSE)

HSE record retention policy 2013.pdf

Appendix 7

Survey Opening Introduction

Survey Introduction.docx

Appendix 8

Deloitte – GDPR Six months on

Deloitte LLP - GDPR six months on.pdf

Appendix 9

Brodies Business Survey on GDPR

Brodies - Business Survey on GDPR (Dec

Appendix 10

Brodies Business Survey on GDPR

Brodies - Business Survey on GDPR (Dec

Appendix 11

Brodies Business Survey on GDPR

Brodies - Business Survey on GDPR (Dec

Appendix 12

Brodies Business Survey on GDPR

Brodies - Business Survey on GDPR (Dec

TABLES

Table 1 - *List of European Countries included in the GDPR regulations 2018*

Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark
Estonia	**Finland**	**France**	**Germany**	**Greece**	**Hungary**	**Italy**
Ireland	**Latvia**	**Lithuania**	**Luxembourg**	**Malta**	**Netherlands**	**Poland**
Portugal	**Romania**	**Spain**	**Slovakia**	**Slovenia**	**Sweden**	**United Kingdom**

Table 2 – *Listing of Awareness levels and respective numbering system used*

Survey Choice	Numbering System
No Knowledge at all	1
Not so Familiar	2
Somewhat Familiar	3
Very Familiar	4
Extremely Familiar	5