An investigation into how a HR department within a Cardiff based company will deal with the changes of the Data Protection Act to the new EU’s General Data Protection Regulation.

A dissertation submitted in partial fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Business Information Systems

by G. Counsell

Department of Computing & Information Systems
Cardiff School of Management
Cardiff Metropolitan University
April 2018
Declaration

I hereby declare that this dissertation entitled ‘An investigation into how a HR department within a Cardiff based company will deal with the changes of the Data Protection Act to the new EU’s General Data Protection Regulation’ is entirely my own work, and it has never been submitted nor is it currently being submitted for any other degree.

Candidate: Gerard Counsell

Signature:

Date:

Supervisor: Taslima Begum

Signature:

Date:
Abstract
All organisations will hold some form of personal data for their employees, which tends to be the responsibility of the HR department. As a result of this, organisations will be required to comply with data protection laws. The current data protection law is the Data Protection Act 1998, however, as of the 25th May 2018, it will be replaced with the General Data Protection Regulation (GDPR) 2018. Consequently, the main aim of the research is to identify the changes under the new regulation and investigate how these changes will impact the HR department within Company X for the research. There were 4 participants within the research, consisting of two HR advisors, one HR business partner and HR manager and the Lead Policy Officer within the Information Commissioners Office (ICO) in Wales. All participants were recruited through the use of non-probability sampling, as selection of participants was at the researcher’s discretion and all information was obtained through the use of both primary and secondary research, in order to understand how the employees have identified the changes between the legislations and what impact this will have on the company and the HR department. In addition to this, all participants were required to read an information sheet prior to participation, as well as read and sign a consent form. The main findings from the research were that the GDPR was announced a while ago, which gives Company X plenty of time to implement changes. In addition to this, the new legislation being put in place is simply to top-up current data protection practices. The department have a range of supporting materials to use to assist with the change and have started to implement the changes necessary in order to be compliant. However, this comes at a cost to finances as well as time. Despite this, the cost of the organisation having to make changes to comply with the GDPR is preferable over the fines that they would be liable for if they were to fail to comply with the new legislation by the given date. Furthermore, the research project was conducted on a fairly large-scale organisation and therefore findings may not apply to smaller organisations. As a result of this, further research would need to be conducted in order to determine how smaller organisations are coping with the changeover from the Data Protection Act 1998 to the GDPR.
Acknowledgments

I would like to give thanks to my family, friends, girlfriend and my dissertation supervisor Taslima Begum for all their help and support they have given me during the duration of my dissertation.

I would also like to thank all the participants who took part in the research for giving up their time to help with the data collection process.
## Contents

Declaration ............................................................................................................................ ii 

Abstract ............................................................................................................................... iii 

Acknowledgments ................................................................................................................. iv 

Table of Figures ..................................................................................................................... vii 

1.0 Introduction ................................................................................................................... 1 

2.0 Purpose of the Study ....................................................................................................... 3 

2.1 Aim ............................................................................................................................... 3 

2.2 Objectives ..................................................................................................................... 3 

3.0 Literature Review .......................................................................................................... 3 

3.1 Introduction .................................................................................................................. 3 

3.2 Data Protection Act 1998 ............................................................................................. 4 

3.2.1 Information Commissioner’s Office ...................................................................... 5 

3.2.2 Conclusion ............................................................................................................. 5 

3.3 General Data Protection Regulation ............................................................................ 6 

3.4 Changes from the Data Protection Act 1998 to the General Data Protection Regulation ...... 8 

3.4.1 Accountability ........................................................................................................ 9 

3.4.2 Lawful basis for processing .................................................................................. 13 

3.4.3 Privacy Notices ..................................................................................................... 15 

3.4.4 Subject Access Requests ...................................................................................... 15 

3.4.5 Automated Decision Making ............................................................................... 16 

3.4.6 Data Breaches ........................................................................................................ 16 

3.4.7 Compliance Programme ........................................................................................ 16 

3.4.8 Conclusion ............................................................................................................. 17 

3.5 Ramifications if not compliant with legislations ........................................................... 17 

3.5.1 Data Protection Act 1998 .................................................................................... 18 

3.5.2 General Data Protection Regulation ................................................................... 18 

3.5.3 Case Studies ......................................................................................................... 19 

3.5.4 Conclusion ............................................................................................................. 20 

3.6 Conclusion ................................................................................................................... 20 

4.0 Methodology .................................................................................................................. 21 

4.1 Introduction .................................................................................................................. 21 

4.2 Research Philosophy .................................................................................................... 22 

4.3 Research Approach ..................................................................................................... 23 

4.4 Research Strategy ........................................................................................................ 24
4.5 Research Design ........................................................................................................25
4.6 Data Collection .........................................................................................................25
4.7 Data Analysis Techniques .........................................................................................26
4.8 Ethical considerations ...............................................................................................27
4.9 Research Limitations ...............................................................................................27
5.0 Results .......................................................................................................................28
5.1 Introduction ...............................................................................................................28
5.2 Themes ......................................................................................................................31
5.2.1 Awareness .............................................................................................................31
5.2.2 Changes ................................................................................................................31
5.2.3 Supporting Material ............................................................................................34
5.2.4 Proactive ................................................................................................................35
5.2.5 Impact ....................................................................................................................36
6.0 Discussion ..................................................................................................................37
7.0 Conclusion .................................................................................................................40
8.0 References ...............................................................................................................42
9.0 Appendices ................................................................................................................48
  Appendix A – Ethics Form ............................................................................................48
  Appendix B - Information Sheet for Company X.........................................................52
  Appendix C – Information Sheet for the ICO ...............................................................53
  Appendix D – Consent form Interviewee 1 .................................................................54
  Appendix E – Consent form Interviewee 2 ..................................................................55
  Appendix F – Consent form Interviewee 3 .................................................................56
  Appendix G – Consent Form Interviewee 4 ...............................................................57
  Appendix H – Company X Semi Structured Interview Questions ............................58
  Appendix I - ICO Semi Structured Interview Questions ..........................................59
  Appendix J – Transcript from Interview 1 .................................................................60
  Appendix K – Transcript from Interview 2 .................................................................66
  Appendix L – Transcript from Interview 3 .................................................................71
  Appendix M – Transcript from Interview 4 ...............................................................79
Table of Figures

Figure 1- The Honeycomb of Research Methodology (Jonathan Wilson, 2014, p.8)...........21
Figure 2- Research approaches (Wilson, 2014.p.14).........................................................23
Figure 3- Methodological choice (Saunders, Lewis and Thornhill, 2012.p.165)...............24
Figure 4- Thematic Network of data collection .................................................................30
1.0 Introduction

Scherrer and Scherrer (2010) state that within this information age,

“personal information plays a valuable role in many aspects of an individual’s life. Entities throughout most sectors of society are interested in collecting information and using the information for any of a number of purposes” (Scherrer and Scherrer, 2010, p1).

Safety and Security are paramount in everybody’s lives. This also includes how individuals want their personal information to be kept. This can be supported by Hallinan, Friedewald and McCarthy (2012) who state that the results from the Public Awareness Survey 2008 displayed that the public regarded data protection and privacy as significantly important. Fisher (2013) also states that individuals are entrusting important identifying information to companies, where, most of the time,

“those companies take seriously the obligation to protect our data and prevent it from failing into the hands of those who could use it to benefit themselves at our expense. Some companies, however, fail to do enough to meet that burden” (Fisher, 2013, p215).

This is supported by Alan Calder’s statement that “secure management of personal digital information has become a key organisational challenge for both the public and private sectors in the 21st century’s information age” (Calder, 2010; cited by Jay and Clarke, 2010. p.5.). The main way of keeping personal data secure is through the use of legislations. The core current legislation in place which will be looked at is the Data Protection Act 1998. This act, which implements the Data Protection Directive (96/46/EC), which is an EU legal act of data protection, came into force on the 1st March 2000 and therefore replaced the Data Protection Act 1984 and is currently one of the main legislations used to support data protection. However, there is a new legislation that will replace both the Data Protection Act 1988 and the Data Protection Directive (96/46/EC), called the General Data Protection Regulation (2016/679 EU) (GDPR). This act will be implemented on the 25th May 2018.
Most modern-day companies will now have a department of Human Resources (HR) who are responsible for recruitment, safety, employee relations, training and development, compliance, as well as compensation and benefits. Some of these aspects require the department to keep personal data so that it can be used to assist such processes. Personal data refers to any data relating to a living individual who can be identified from the data or the data and other information which is in the possession of, or likely to come into the possession of the data controller. This can include any expression of opinion about the individual or any indication of the intentions concerning the data controller or any other person in respect of the individual (Legislation.gov.uk, 2017). A data controller can be an individual who alone, jointly or in common with others determines the purposes for which the manner in which any personal data is processed. They are also responsible for ensuring that provisions of the Data Protection Act are complied with (Dft.gov.uk, 2017). The research will evaluate the legislations and identify the key changes which would directly affect the HR department of Company X and how they will manage the change, as well as the potential implications of not complying with the new legislation that will be in place.

1.1 Background Information about Company
Company X was founded in 1979 and operates within the Information Technology and Services industry, with roughly 1000 employees across the UK. They specialise in Business Process Management, Outsourced Loan Servicing, Lending Software, Business Transformation and Business Process Outsourcing. Most of their clients are within the financial services sector. They are a dynamic and growing company with the vision to be the lead provider of software and third-party servicing to financial services and insurance clients.
2.0 Purpose of the Study

2.1 Aim
The aim of the study is to evaluate the EU’s General Data Protection Regulation and highlight the changes from the Data Protection Act and specifically how these changes will impact a HR department in a Cardiff based company in practice.

2.2 Objectives
- Identify current practice of data protection
- Conduct a literature review of key changes of the new legislation
- Assess the effect on a HR departments practices in a UK company
- Critical review of impact
- Detail the legal implications if GDPR not followed correctly. Outcome differential compared to the Data Protection Act 1998.

3.0 Literature Review

3.1 Introduction
Human Resource Management can be defined as a

“strategic and coherent approach to the management of an organisations most valued assets - the people working there who individually and collectively contribute to the achievement of its objectives” (Armstrong, 2006.p.3).

To achieve this approach, a HR department are required to collect data relating to their employees, known as HR records. The Chartered Institute of Personnel and Development (CIPD), which is a professional association for human resource management professionals, stated in 2017 that HR records consist of a wide range of data that relates to individuals working within an organisation, with the examples of pay or absence levels and hours worked. They state that the information tends to be stored electronically but may include paper records as well. The CIPD states that the Data Protection Act 1998 applies to most personal records in either paper or digital format, therefore this would apply to the General Data Protection Regulation.
Elizabeth Denham, the UK Information Commissioner who is in charge of data protection enforcement in 2017, stated that the General Data Protection Regulation is a step change for data protection and that it is still in evolution. Additionally, she states that for companies who already comply with the existing data protection laws, the new regulation is only a step change (ico.org.uk, 2017). The ramifications if a company doesn’t comply with the legislations aren’t unknown, with the legislations detailing the outcome supported by real life examples of companies that don’t comply.

3.2 Data Protection Act 1998

The Data Protection Act 1998 repealed the Data Protection Act 1984 and implemented the Data Protection Directive with the purpose of giving protection and laying down the rules about how personal data can be used and is currently the main data protection legislation. It was created to protect the misuse of personal data. The act applies to any data processing which includes obtaining, recording, holding or carrying out any operations on the data within the UK. The 1998 act was closely modelled on the 1984 act, as well as being aligned with EU laws. However, there were some minor changes, such as the act now applying to both paper and digital based information. The act also differed with various new broader definitions such as data, processing and data controller.

The act consists of eight principles which Carey (1998) refers to as the backbone of the legislation. The principles outline the requirements a data controller must meet in order to be compliant. Company X needs to comply with all eight principles and as a HR department they would need to comply with the Act when completing various tasks. Failure to comply can result in huge ramifications for the company. The principles are:

- Personal data shall be processed fairly and lawfully and shall not be processed unless—
  - (a) at least one of the conditions in Schedule 2 is met, and
  - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
• Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

• Personal data shall be accurate and, where necessary, kept up to date.

• Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

• Personal data shall be processed in accordance with the rights of data subjects under this Act.

• Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

• Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (ico.org.uk, 2018).

3.2.1 Information Commissioners Office
The Information Commissioners Office (ICO) are a UK independent body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals (ico.org.uk, 2018). They are the regulator for the Data Protection Act 1998, therefore if there is any non-compliance, they have various methods in place to correct that, with the possibility of issuing monetary penalties. Data controllers are required under the Act to register with the ICO, whereby they will disclose the information of the processing of data.

3.2.2 Conclusion
Company X are required to comply with all eight principles of the Data Protection Act 1998. There may be principles that are more predominate for the HR department due to the tasks they are responsible for. Nonetheless, they must comply with all eight. Failure to do so will be a breach of the Data Protection Act 1998 and will face action by the ICO.
3.3 General Data Protection Regulation

The General Data Protection Regulation (2016/679 EU) (GDPR) is the new governing legislation for collecting and processing personal data in the EU. It will come into effect on May 25th, 2018 for all EU member states, including the UK which will still be a member of the EU at the time. The GDPR will continue to apply within the UK after Brexit due to it being incorporated into UK law by the European Union (Withdrawal) Bill. The Government has also published the Data Protection Bill, which will supplement the GDPR, replacing the Data Protection Act 1998. The head of the Information Commissioner’s Office, Elizabeth Denham, stated in a speech at the Institute of Directors Digital Summit in October 2017 that

“we have a digital infrastructure that was unimaginable when the Data Protection Act was forged 20 years ago” (Ico.org.uk, 2017).

Patrick O’Kane (2017) supported this, stating that the last time EU data privacy laws majorly changed was in 1995. The GDPR gives specific new obligations for organisations to meet compared to previous laws. Elizabeth Denham further says

“the real change for organisations is understanding the new rights for consumers and citizens. The GDPR is an evolution of the current law and a step change that brings greater accountability, transparency and consumer control and these are the pillars of data protection law that will give people agency over their information” (Ico.org.uk, 2017).

To support this, Peter Blume stated that the GDPR will be “an important step in the maturing of data protection law. It brings the law up to date and it is likely that it will sustain good or at least better actual protection” (Blume, 2014, p.276).

Under the GDPR, the data protection principles set out the main requirements for organisations, however there are now six principles compared to the original eight under the Data Protection Act 1998. Article 5 of the GDPR requires personal data shall be:
• “a) processed lawfully, fairly and in a transparent manner in relation to individuals;

• b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

• c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

• d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

• e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

• f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles” (ico.org.uk, 2018).

The GDPR applies to any organisation which processes data of any EU citizen regardless of where the processing is taking place, therefore offers a much wider scope in comparison to previous data protection laws. As mentioned, the Government has published the Data Protection Bill 2017, which will supplement the GDPR and replace the Data Protection Act 1998.
3.4 Changes from the Data Protection Act 1998 to the General Data Protection Regulation

Elizabeth Denham (2017) has stated that for companies which already comply with the existing data protection laws, the GDPR is only a step change. Therefore, there are similarities between the two pieces of legislations, however there are also new obligations under the GDPR which companies must adhere to. Companies must look to address these new obligations and ensure that they are compliant by the 25th May 2018.

Qian Mou (2017) states that one of the initial responsibilities for HR in GDPR compliance will be to identify employee personal data, where it is stored and how it’s used. This is supported by Patrick O’Kane (2017) who stated that to implement GDPR, organisations must understand where their data is coming from, as well as how it is used. A method which can be used to help these findings is often known as a data audit or data map (XpertHR, 2017). Patrick O’Kane defines a Data Audit as a:

“process by which you obtain evidence about how data is being processed across your company to identify whether the company is behaving in a way that is compliant with data protection law and regulation” (O’Kane, 2017.p.22).

Patrick O’Kane (2017) further claims that the audit will provide an organisation with an inventory of their data, which will help them to prepare a data map and a data flow diagram. Qian Mou (2017) states that a data map starts by looking at personal data from job applicants and carries through the employment lifecycle. She also said there isn’t a prescribed format for the data map and it may come in a variety of different forms, as long as it achieves the purpose of helping the organisation identify what personal data is collected, where its stored and its processed. Patrick O’Kane (2017) breaks the process into two steps whereas Qian Mou (2017) merges the process, known as either a data audit or data map. Firstly, the data audit is used to get an understanding of how your company uses data and changes needed to be made to comply with the GDPR.
O’Kane states that there are many tools available to help conduct an audit. He gives the example of using questionnaires to collect the majority of the information, however you would still be required to go and speak to people. The second stage is creating a data map, which he refers to as a “like a treasure map, only more valuable” (O’Kane, 2017.p.41). A data audit will yield a wealth of information, but the information isn’t organised, which is why you need a data map to organise this raw data. Qian Mou (2017) states that the data map can be used as a compliance of the GDPR, requiring a detailed record to be kept of personal data processing activities if the map contains the necessary information. She also stated that, very importantly, it can identify gaps between the current practice and the requirements under the GDPR.

3.4.1 Accountability

The European Data Protection Supervisor states that the GDPR integrates accountability as a principle which requires that

“organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested” (European Data Protection Supervisor, 2018).

The ICO state that this is detailed in article 5(2), which McKean and Gibson (2018) state is one of the biggest changes under the GDPR. O’Kane (2017) says that organisations must be able to show and not tell the regulator how you are complying with the GDPR.

Under the principle, employers are now required to keep extensive internal records of data processing operations, this must be available to be produced to the supervisory authority for inspection on request. McKean and Gibson (2018) state that employers should create a data register to meet their record keeping requirements. This should be an up to date written record containing information about personal data processed by the organisation. The ICO state that in order for organisations to comply they must:

- implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;
- maintain relevant documentation on processing activities;
- where appropriate, appoint a data protection officer;
- implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
  - data minimisation;
  - pseudonymisation;
  - transparency;
  - allowing individuals to monitor processing; and
  - creating and improving security features on an ongoing basis.
- use data protection impact assessments where appropriate (ico.org.uk, 2018).

McKean and Gibson (2018) also advised employers to keep records of the legal bases for processing the data as well any legitimate interests relied on for processing activities linked with the data and the location of the data.

### 3.4.1.1 Record Keeping
The accountability principle requires Company X to keep extensive internal records of data processing as well as relevant documentation on processing activities which can be done through creating a personal data register. As Qian Mou (2017) mentioned, the information generated from the data map can be used to create the personal data register, although in order to keep the records up to date Company X should review their policies and processes to ensure that the register is updated when there are changes to organisational data processing practices.

### 3.4.1.2 Data Protection Officer
Under the principle companies may be required to appoint a Data Protection Officer (DPO) if they are a public authority, carry out large scale systematic monitoring of individuals, or carry out large scale processing of special categories of data or data relating to criminal convictions and offences (ico.org.uk, 2018). Company X would be required to appoint a DPO as they are likely to carry out both large scale processing of special categories as well as monitoring of
individuals. O’Kane (2017) stated there are also time and cost savings by appointing a DPO due to them having the expert knowledge, so being less likely to require outside information which would cost the company, as well as all data protection queries being able to be sent to the DPO and not be bounced back and forth. He also states that by having a DPO a company will more likely have GDPR controls in place. Policies, procedures and training are more likely to be completed if a DPO is in place.

3.4.1.3 Policies
O’Kane (2017) states that companies may not have to change their policies but with GDPR changing the rules on how you can process data it will likely be that company policies will need to be updated. He says that as part of the accountability principle companies are expected to put in place appropriate corporate governance around personal data, where he states having appropriate policies in place is a big part of this. He mentioned policies such as a data protection policy, data retention policy and data breach policy. Company X are most likely to already have these policies in place but there is a need to go through them and possibly amend them to fall in line with GDPR.

3.4.1.4 Data protection by Design and Default
McKean and Gibson (2018) define data protection by design and default as a

“new approach to data that will require organisations to embed privacy considerations in both operational and strategic HR” (McKean and Gibson, 2018).

Cavoukian (2011) states that Privacy by Design is an approach characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. The aim of it is to prevent any data breaches occurring. McKean and Gibson (2018) state that it requires employers to take data protection risks into account throughout the process of designing and operating a policy, product, process or service. They state it requires employers to assess and implement appropriate and proportionate technical and organisation measures and procedures in place so that the processing of data complies with the GDPR.
Whereas Cavoukian (2011) states that the approach to privacy by design is that if an individual does nothing, their privacy still remains intact. There is no action required by the individual to protect their privacy, it’s done by default. McKean and Gibson (2018) state that employers need to put mechanisms in place within their organisation to ensure that the personal data that is processed is necessary for each specific purpose. Cavoukian (2011) said this can include:

- **Purpose Specification** – the purpose or purposes for which personal information is collected, used, retained and disclosed will be communicated to the data subject at or before the time the information is collected

- **Collection Limitation** – only the personal data that is needed is collected and processed for a specific purpose

- **Data Minimisation** – collection of personally identifiable information should be kept to a strict minimum.

- **Use, Retention, and Disclosure Limitation** – the use, retention and disclosure of personal data will be limited to what is necessary for each purpose. Data will only be retained for as long as necessary to meet the purpose then after that will be securely destroyed.

Company X and the HR department are likely to have measures in place to address the concerns of retention as well as data being processed for a specific purpose as these come under the principles of the Data Protection Act 1988. However, with the new principle of accountability under the GDPR there are obligations to take technical and organisational measures when processing data and the ability to show how you comply with the obligation.

**3.4.1.5 Data Protection Impact Assessment**

Tankard (2016) states that data impact assessments will

“be required where processing of data is deemed to be high risk for the rights and freedoms of the data subjects involved” (Tankard, 2016, p. 5).
The GDPR requires organisations to carry out Data Protection Impact Assessments (DIAs) if they plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale (Consultation: GDPR DPIA guidance, 2018).

Also, Article 35(4) states that the ICO is required to publish a list of types of processing that they would consider likely to be a high risk which would require the use of a DPIA. The HR department are highly likely to have to complete a DPIA due to the processing of special category of data on a large scale. Tankard (2016) states that the assessment must detail the safeguards, security measures and mechanisms that are in place for address risk and ensuring compliance. O’Kane (2017) states that the assessments are evidence that a company takes data privacy seriously as well as being evidence if a regulator visited.

3.4.2 Lawful basis for processing

Under the GDPR there has been a modification of the requirement to have a lawful basis in order to process personal data. The ICO states that it replaces and mirrors the previous requirement to satisfy one of the ‘conditions for processing’ under the Data Protection Act 1998. However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing (ico.org.uk, 2018).

Article 6 under the GDPR details six lawful bases of processing and article 9(2) details the conditions in order to process special category data. The same process applies under the Data Protection Act 1998 with Schedule 2 and 3.
3.4.2.1 Consent

Consent under the Data Protection Act 1998 could be obtained via tick boxes or as part of the terms and conditions of a contract. However, the GDPR sets a higher standard for consent. The definition of consent in Article 4(11) of the GDPR is similar to the old definition, adding some detail on how consent should be given, defined as:

“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (Consultation: GDPR consent guidance, 2017).

The GDPR gives more emphasis with the indication having to be unambiguous and involve a clear affirmative action. There are also more changes, such as the organisation must have clear records to demonstrate consent and they also need to inform people that they have a right to withdraw, as well as offering easy ways to do this. McKean and Gibson (2018) stated that many employers process employee personal data based on consent. However, with the GDPR introducing stricter requirements for valid consent, employers can no longer rely on broad consents in employment contracts as a way of processing employee personal data. Furthermore, with the requirement that consent must be freely given, it would generally be difficult to obtain in the employment context due to the imbalance of power (McKean and Gibson, 2018). They stated that three-legal basis which can be relied upon is that processing is necessary for:

- Compliance with a legal obligation;
- The performance of a contact; or
- The purposes of the legitimate interests of the employer or a third party (McKean and Gibson 2018)

The HR department would need to review their legal basis for processing and must adapt to the change in order to comply with the GDPR. Qian Mou (2017) stated that the data map can be useful to identify these gaps and alert the organisation to the changes that need to be made (XpertHR, 2017). Broadbent (2018) states that if an employer relies on the legitimate
interests ground to process employee data, employees have the right to object to the processing. This supports McKean and Gibson (2018) advising that an organisation should keep a record of the legitimate interests relied on for processing activities.

3.4.3 Privacy Notices
Under the GDPR, employers will be required to provide more detailed information in comparison to the Data Protection Act 1998 to employees and job applications about the processing of their personal data. Employers tend to provide this information through the use of information notices, also known as privacy notices. The GDPR requires the organisation to include various information that the department would need to comply with. It also states that employers must provide the information at the point of data collection. As well as, if the employer wishes to process existing data for a new purpose, they must give information to the employee or job applicant for further processing. The HR department will most likely need to send out privacy notices to employees with the new information. In addition to this, with the department most likely changing their legal basis for processing, they are required to detail that information, therefore employees will need to be updated.

3.4.4 Subject Access Requests
Subject access requests aren’t a completely new requirement under the GDPR as they already exist under the principle of a data subject rights within the Data Protection Act 1998. However, what the GDPR does is require organisations to provide the requested information without undue delay. The information must be provided to the data subject within one month of the request or three months if the case is complex. The GDPR places more rigorous obligations on employers to ensure that there are systems in place to ensure that they comply with access rights, with particular emphasis placed on the clarity, transparency and accessibility of such systems (McKean and Gibson, 2017). Also under the GDPR a data subject access request is free of charge, unless the request is manifestly unfounded or excessive. Previously organisations were allowed to request a fee under the Data Protection Act 1998.
3.4.5 Automated Decision Making

McKean and Gibson (2018) state that employees have a right under the GDPR not to be a subject to a decision made solely by automated processing where that decision sufficiently affects them. Examples of this can be recruitment, performance management/triggers for sickness absence, attendance bonuses, holiday or shift rostering and employee monitoring. The GDPR does contain exceptions to this rule when the automated processing is based on explicit consent or where it is necessary for entering into or performing the employment contract. If an employer does rely on the exception to the rule, there must be additional safeguards, including the right for an employee to require human intervention in the processing, to express a view and to contest the decision.

3.4.6 Data Breaches

Under the GDPR organisations must report any data breaches to the ICO within 72 hours of becoming of the breach. The regulation also states that if the breach is likely to result in a high risk of adversely affecting individual’s rights and freedoms, the organisation must also inform those individuals as soon as possible. The ICO suggest that organisations have a robust breach detection, investigation and internal reporting procedures in place. They state this can help the decision making about whether or not you would need to notify the ICO and the individuals affected (ico.org.uk, 2018). Organisations are also required to record any data breaches, regardless of if they were needed to notify.

3.4.7 Compliance Programme

In order for Company X and the HR department to be compliant by the 25th May 2018, they should develop and implement a compliance programme. DLA Piper, a global law firm, stated that key features of the implementation of a compliance programme are to:

- Assemble a project team;
- Assess potential areas of exposure in current working processes;
- Develop a clear plan of action to be ready for 2018;
- Implement changes needed in a logical/prioritised manner; and
- Establish an effective information governance framework to manage risk (Dlapiperbeaware.co.uk, 2018).
Company X and the HR department should have a compliance programme in place as this will help with the changeover in legislation, however McKean and Gibson (2018) do state that the implementation of a GDPR compliance programme requires a substantial investment of money, organisational resources and management time. It is also vitally important for the company and department to gain board and senior management level buy in so that compliance will be across the organisation and be in place by the 25\textsuperscript{th} May 2018.

3.4.8 Conclusion

There are various changes due to the implementation of the GDPR. This section looked at identifying the main changes which relate to and need to be addressed by the HR department at Company X. There are various tools, guides and techniques out there which can help the organisation and department with the process. McKean and Gibson in 2018 state that:

“It is important for employers to take a realistic, risk-based approach to compliance. The implementation of a structured programme will assist in mitigating the risk of a fine and reducing the severity of any infringements. Employers should aim to be compliant by 25 May 2018, but this may be challenging in practice, so they should focus on the most important and riskiest areas first” (McKean and Gibson, 2018).

They suggest conducting an initial audit and risk assessment, with the next step being to develop and implement a GDPR compliance programme. The programme would include a timeline for completing the compliance activities which have been set out by the organisation. The team should prioritise based on highest risk and most impact. Organisations may need to adjust initial estimate on the time frame once started.

3.5 Ramifications if not compliant with legislations

This section will detail the possible ramifications an organisation could face under both the Data Protection Act 1998 and the GDPR. It will also look at past examples of breaches under the Data Protection Act which are relevant to a HR department setting. Due to the GDPR not being implemented, there are no previous examples, only what the legislation states will happen as a result of breaching the GDPR.
3.5.1 Data Protection Act 1998

An employee can apply to the ICO for an assessment as to whether or not any personal processing by their employer has been, or is being, carried out in compliance with the Data Protection Act 1998. If the ICO is satisfied that an employer has contravened, or is contravening, any of the eight data protection principles, they may serve an enforcement notice. Failure to comply with the terms of any such notice is an offence of which the penalty on summary conviction is an unlimited fine (Stibbs, 2018).

From the 6th April 2010, the ICO, under section 55A and 55B of the Data Protection Act 1998, has the power to order organisations to pay up to £500,000 as a monetary penalty in the event of a serious breach of any of the data protection principles by a data controller. Nicky Stibbs (2018) states that the ICO may impose a monetary penalty if satisfied that:

“the breach is likely to cause substantial damage or distress; the breach was deliberate; and the data controller knew or ought to have known that there was a risk that the breach would occur and was likely to cause substantial damage or distress, but failed to take reasonable steps to prevent it” (Stibbs, 2018).

Furthermore, Stibbs (2018) claims that the ICO has stated that a pragmatic and proportionate approach will be adopted in relation to the issue of monetary penalties, and an organisation's size, financial resources and the severity of the breach committed will all be considered.

3.5.2 General Data Protection Regulation

Patrick O’Kane states that the GDPR’s penalties “strike fear in the heart of executives and boards” (O’Kane, 2017. p.3). He states that there are huge penalties put in place under article 83 of the GDPR if organisations fail to comply with the regulation. Under the GDPR there are two levels of fines. The first one is fines of 2% of global annual turnover or €10 million, whichever is higher, for administrative breaches, such as failing to appoint a Data Protection officer or breaching consent rules. The second fine, being the maximum, is 4% of global annual turnover or €20 million, whichever is higher. These fines will usually relate to a breach of a data subject’s rights or any of the basic GDPR principles (O’Kane, 2017). Patrick O’Kane (2017) also states that regulators aren’t free to fine as much as they want for any GDPR breach, however under article 83 of the GDPR it states that fines must be proportionate to the breach.
itself. O’Kane (2017) also states that he suspects major fines will be reserved for major data breaches.

3.5.3 Case Studies

In 2016 Hampshire County Council was fined £100,000 after files containing highly sensitive personal details of more than 100 people were discovered in a disused building. Social care files were found along with 45 bags of confidential waste. The documents which were found contained “highly sensitive” information about adults and children in vulnerable circumstances, according to the ICO (Press Association, 2016). The ICO goes on to state that:

“the council failed to take appropriate organisational measures against unauthorised processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 of the DPA” (Hampshire County Council Monetary Penalty Notice, 2016).

They also state that the fifth data protection principle at Part I of Schedule 1 to the Data Protection Act was also contravened by the council, in that data was kept for longer than necessary for its purposes.

Another case study was in 2011, whereby Powys Council were fined £130,000 for a child data error fine. Two separate reports about child protection cases were sent to the same shared printer, and it is thought two pages from one were mistakenly picked up. It was believed that the mistakenly picked up pages were then sent out without being checked. The recipient received the correct report with two additional pages, containing the identities of the parent and child whose personal details were included in the papers. The fine at the time was the greatest issued out by the ICO and again shows a breach of the 7th principle, with the error displaying lack of technical and organisational measures put in place by Powys Council (BBC News, 2011).
3.5.4 Conclusion
There is a huge increase from the maximum fine under the Data Protection Act, being £500,000, to €20 million or 4% of an organisation's global annual turnover under the GDPR. These new fines can have a huge impact on organisations in the present and the future. Looking at past examples of enforcement, the higher fines under the Data Protection Act 1998 were more linked to the unauthorised access to personal data which can be referred to as 'hacking'. Although company X would need to comply with this, it would more likely be in the control of their IT/Security department. Therefore, the case studies found which can be relevant to the HR department, saw fines nowhere near the maximum under the Data Protection Act. However, under the GDPR, the HR department is at risk of receiving both levels of fines, the first being the lower one which can be for administrative breaches, and the second being if the HR department fail to comply with a data subject's rights or any of the principles.

The HR department plays a big part in the compliance of the GDPR with the employee data they have stored however they are more likely to now incur huge penalties if they fail to comply with the GDPR. The Veritas 2017 GDPR report supported this, by surveying 900 senior business decision makers in 2017 across the globe, concluding that 21% of them are very apprehensive about the potential layoffs, fearing that staff reductions may be inevitable as a result of financial penalties incurred with the result of non-compliance of the GDPR. There are also worries about their brand images as a consequence of noncompliance (Veritas GDPR Report, 2017).

3.6 Conclusion
The literature review details the current data protection practices under the Data Protection Act 1998 and how the HR department is required to comply with the eight principles. There is more emphasis on certain principles in the department as certain principles may come under other departments' responsibilities. There was a clear need for a new and up to date legislation due to the growth of personal data and how it can be used through technology. Therefore, the GDPR was introduced. Under the GDPR there are various changes. Some of these directly impacted the HR department, therefore they need to know what they must do in order to comply with the regulation. Broadbent (2018) stated that compliance with the GDPR is not a “one-size-fits-all” approach and will depend on a wide range of factors,
therefore it will require the HR department and Company X to apply themselves to the principles under the GDPR in order to meet compliance. There were various tools, materials and techniques available to support organisations through this change. There is a huge importance to comply with the GDPR due to the vast ramifications if an organisation were to fail to comply with the legislation. However, there is also a growing concern that organisations may fail to be fully compliant under the GDPR when it goes live on the 25th May 2018. Alex Brown states that “no big business is going to be fully compliant. It is impossible” (IFLR Correspondent, 2017). The same concern arose with the Data Protection Act with the NCC, an independent consultancy body, stating that they believed many businesses are not aware of the changes from the 1984 to the 1998 act as well as the implications (UK companies unprepared for new data protection act, 1999).

### 4.0 Methodology

#### 4.1 Introduction

This section will detail the purposed research methodology for the study. Jonathan Wilson states that “understanding research, methodology and methods is an essential requirement to your project” (Wilson, 2015, p.1). To do that he introduces the ‘Honeycomb of Research Methodology’, which consists of six main elements that combine to make up the centre segment – research methodology, which can be shown in Figure 1.

![Figure 1- The Honeycomb of Research Methodology (Jonathan Wilson, 2014, p.8)](image-url)
Wilson (2004) states this approach is different in comparison to several other research methods. Other methods tend to be in the form of either a linear-type diagram, or a series of layers. He says whilst these types of methods are ideal for highlighting the elements identified in the honeycomb, they often fail to address some key issues. One being that although a methodology chapter does follow a structure, the researcher may not consider each element in the order that is structured within the chapter, therefore the honeycomb not only numbers each segment to show the typical structure but it recognizes that the process may not be linear, which can be seen through the six outer segments combing to make up the centre segment. Another issue is that other research methods do not show the relationship or link between each segment. Finally, all elements are not always considered when writing a research methodology chapter. Consequently, the honeycomb was selected to help construct the research methodology for this research project.

4.2 Research Philosophy

Jonathan Wilson (2004) said that having an understanding of research philosophy is important because it is fundamental to how you approach your research. Mark Easterby-Smith et al. (2002) states that there are at least three reasons why an understanding of philosophical issues is very useful. Firstly, it can help clarify research designs. Secondly, a knowledge of philosophy can help the researcher to recognise which designs may or may not work. Lastly, philosophy can help the researcher identify and adapt research designs according to the constraints of different subject or knowledge structures. By having an understanding of research philosophy, it can help the researcher to think about their own role within the study. There are various research philosophies which can be adopted by the researcher, but the adopted philosophy is Interpretivism. Jonathan Wilson states that this philosophy supports the view that the researcher must enter the social world of what is being examined. They do this by analysing the social actors within their own cultural setting which tends to be qualitative and subjective in nature (Wilson, 2014). This can be supported by Hussey & Hussey who state that the assumption is that by placing people in their social contexts, there is a greater opportunity to understand the perceptions they have of their own activities (Hussey & Hussey, 1997). This emphasises the difference between conducting research among people rather than about objects such as trucks and computers (Saunders, Lewis and Thornhill, 2012).
The aim of this research is to evaluate how the change in legislation directly impacts a given/specific HR department and how they adapt to these changes, therefore the researcher will engage with the organisation and interpret the views and opinions of respective social actors to help achieve the objectives of the report. As a result, the research philosophy most appropriate would be interpretivism.

4.3 Research Approach

Research methods are often grouped into two approaches, inductive and deductive. Both approaches can be seen in Figure 2.

![Figure 2- Research approaches (Wilson, 2014.p.14)](image)

Saunders, Lewis and Thornhill (2012) state that you would use a deductive approach if the research starts with theory and design a research strategy to test the theory, whereas an inductive approach is used if the research starts by collecting data to explore a phenomenon and you generate or build theory, which is often in the form of a conceptual framework. The selected approach for this research project would be the inductive approach. The report will look to gain findings from the knowledge and views of the employees within company X and try to identify themes and patterns and create a conceptual framework.
4.4 Research Strategy

Strategy tends to refer to a plan of action to achieve a goal. Saunders, Lewis and Thornhill, 2012 states

“a research strategy may therefore be defined as a plan of how a researcher will go about answering her or his research question” (Saunders, Lewis and Thornhill, 2012.p.173).

There are two main research strategies which are qualitative and quantitative, each consisting of various methods. This can be shown in Figure 3, which also shows that a researcher may combine the two strategies or possibly use multiple quantitative or qualitative methods within the study.

![Diagram of Methodological choice](image)

**Figure 3- Methodological choice (Saunders, Lewis and Thornhill, 2012.p.165)**

Saunders, Lewis and Thornhill (2012) state that one way of differentiating quantitative research from qualitative research is to distinguish between numeric data and non-numeric data. Quantitative research is often used as a synonym for any data collection technique such as questionnaires, or data analysis such as graphs or statistics that generates or uses numerical data. Qualitative research is often used as a synonym for any data collection technique such as an interview or data analysis, such as categorising data that generates non-numeric data. The research strategy adopted for the research project is a mono-method qualitative study consisting of interviews only. With the aim of the project being to see how the change in legislations impact the HR department of a company, interviews can be seen as the most appropriate method to understand the impact through the opinions and views of
the employees. This also supports the research philosophy and approach, with Denzin and Lincoln (2005) saying that qualitative research is associated with an interpretive philosophy. In addition to this, Saunders, Lewis and Thornhill (2012) state that many varieties of qualitative research commence with an inductive approach. This ties in with the honeycomb, with the first three components being highlighted, whereby Wilson (2014) states the choice of philosophy will likely determine your research approach and strategy.

4.5 Research Design
With the aim of the research project being to see how the new legislation changes impact the HR department and how they will adapt to these changes, the research design would need to be a case study. Collis and Hussey (2014) define a case study as

“a methodology that is used to explore a single phenomenon (the case) in a natural setting using a variety of methods to obtain in-depth knowledge” (Collis and Hussey, 2014.p.68).

Esisenhardt and Graebner (2007) support this by saying a case study design will be relevant if the researcher wishes to gain a rich understanding of the context of the research and the processes being enacted. Saunders, Lewis and Thornhill (2012) also state that a case study design has the ability to generate answers to the question ‘why?’, as well as ‘what?’ and ‘how?’ questions.

4.6 Data Collection
The data for the research project will be collected through the use of interviews, which are a qualitative research method for collecting data, whereby selected participants (the interviewees) are asked questions to find out what they do, think or feel (Collis and Hussey 2014). Using an interpretivism philosophy, interviews will look to explore:

“data on understandings, opinions, what people remember doing, attitudes, feelings and the like, that people have in common” (Arksey and Knight, 1999.p.2).

The purpose of conducting interviews is so that the researcher is able to ask purposeful and concise questions to help collect valid and reliable data that can help the research project. A sampling technique will be applied to the interviews. Techniques can be split into two
categories, probability and nonprobability. Probability sampling refers to participants being selected randomly and the probability of being selected is determined ahead of time by the researcher. Whereas, nonprobability sampling is where the inclusion or exclusion of participants in the sample is left to the discretion of the researcher (Hair Jr et al., 2015). There are also various different types of both probability and nonprobability which the researcher can use. The sampling technique which will be used for the project is the judgement sample, sometimes referred to as a purposive sample, this technique is a nonprobability approach. The technique involves selecting participants in the sample for a specific purpose, where the researcher’s judgement is used to select the sample participants. Participants are chosen because the researcher believes they represent the target population (Hair Jr et al., 2015). The participants are selected based on their job roles within the company or industry. The researcher will look to interview participants which work within the HR department of the case study company, such as HR advisors and Business Director, as well as a participant which work for the Information Commissioners Office, due to their involvement within the data protection industry. The sample size will be 4-6. These participants have been selected due to them being able to help the researcher address the aim and objectives of the research. The interviews would follow a semi-structured approach, consisting of the researcher preparing some questions to encourage the interviewee to talk about the main topics of interest and develop other questions during the course of the interview (Collis and Hussey 2014). There would be two interview sheets, one for the Information Commissioners Office participants and another sheet for the HR department participants, each interview containing four topics with 3-5 questions in each, as seen in appendices H and I. The questions will often be open ended, with the occasional closed question, as this allows the participant to give their opinion and not be restricted in their answers. The interviews would be face to face and recorded so that the researcher can create a transcript to be used to help them analyse their findings.

4.7 Data Analysis Techniques

Hair Jr et al., (2015) states that the objective of qualitative data analysis is to identify, examine, compare and interpret patterns and themes. Clarke and Braun (2016) defines thematical analysis as

“a method for identifying, analysing and interpreting patterns of meaning (themes) within qualitative data (Clarke and Braun, 2016.p.297).
Clarke and Braun (2016) state that thematic analysis can be used to analyse both small data sets (case study) and large data sets (60+ participants). They also state that the analysis provides a framework for organising and reporting the researcher analytic observations. The aim of thematic analysis is not simply to summarise, but to identify and interpret the data collected from the interviews. Thematic analysis looks to identify patterns within and across data in relation to participant’s experiences, views and perspectives, behaviour and practices. Therefore, this choice can help the researcher to understand how the change in legislation has directly impacted the HR department through the analysis of the employees working within the department.

4.8 Ethical considerations

Collis and Hussey (2014) state that the term ethics refers to

“the moral values or principles that form the basis of a code of conduct” (Collis and Hussey, 2014.p.30).

It is essential for the researcher to ensure that all appropriate ethical considerations are applied to the processes of accessing, collecting, analysing and reporting the data. The main ethical considerations will be looking at the collection and analysing of the primary data. All interviewees will receive a copy of an information sheet outlining the aim and objectives of the study, as well as a consent form for the interviewee to sign so that the researcher has the permission to use the information for the project. All interviewees have the right to anonymise themselves and can withdraw within 7 days of the interview. All the information will remain confidential and safely secured and stored. The information will also be destroyed after 30 days. The researcher would also remain non-bias and remain neutral for all data collected.

4.9 Research Limitations

With the research design being a case study, the project is heavily reliant on the involvement of the participants within Company X. The people selected have been chosen based on their job role, experience and knowledge, therefore if they were not willing to participate it could alter the findings of the project, or if they withdraw it could put the whole project at risk as the researcher would be required to find a new sample of participants. Another limitation is
that employees of the company may not answer truthfully as this could portray the company in a negative way, so the researcher may need to take into the account the reliability of the information. The researcher has taken appropriate measures to minimise these risks by providing participants with as much information as possible, through the use of information sheets and a consent form stating what the researcher can do with the collected data, which the participant must sign, as well as all questions being approved by Cardiff Metropolitan University ethical committee.

5.0 Results

5.1 Introduction
The results of the project were generated through the use of thematic analysis. The analysis took place on all four interviews which can be seen in appendices J, K, L & M. Nowell et al (2017) states that the analysis follows six phases:

- Familiarising yourself with your data
- Generating initial codes
- Searching for themes
- Reviewing themes
- Defining and naming themes
- Producing the report

The researcher used the format of phases to help generate the results of the research. The participants of the interviews were two HR Advisors and one HR manager and business partner of Company X, as well as Bethan Bonsall, who is the Lead Policy Officer for the ICO Wales. The researcher ensured that they were familiar with all transcripts by reading them multiple times and the process of coding began by working through each transcript on a line by line basis, highlighting any interesting concepts or phrases. Once all transcripts were coded, a table of all codes, as well as interview numbers was produced and any codes which could generate a theme were highlighted.
Clarke and Braun (2016) stated that

“codes are the smallest units of analysis that capture interesting features of the data (potentially) relevant to the research question” (Clarke and Braun, 2016, p.297).

They go on to say that codes are the building blocks for themes. Figure 4 shows the thematic network which consists of themes and sub-themes generated from the interviews. Attride-Stirling (2001) defined thematic networks as

“web-like illustrations that summarize the main themes constituting a piece of text. The thematic networks technique is a robust and highly sensitive tool for the systematization and presentation of qualitative analyses” (Attride-Stirling, 2001, p.385).
The impact the GDPR has had on Company X and the HR department

5.2.1 Awareness

5.2.2 Changes

5.2.2.1 Not a drastic change

5.2.2.2 Current data protection practices

5.2.3 Supporting Material

5.2.3.1 Internal Support

5.2.3.2 ICO Guidance & Support

5.2.3.3 External Support

5.2.4 Proactive

5.2.5 Impact

5.2.5.1 Cost

5.2.5.2 Time

5.2.5.3 Identified Changes

Figure 4- Thematic Network of data collection
5.2 Themes

5.2.1 Awareness
This theme identifies the awareness around the GDPR. It is not a regulation that has come out to try and catch organisations out but it has given organisations the opportunity to make the changes needed so that they will be compliant by the 25th May. All employees when asked the question “when did you first hear about the change in legislation?” stated that they were aware of the change at least a year ago, if not longer in some instances, as well as the company setting up a GDPR project team around that time. All interviewees were also aware of the change of increased fines as well two of them being aware that data processors are now personally liable. Bethan Bonsall supported this by stating that the ICO have had a 12-step guide for the GDPR on their website for the last two years, as well herself going out and giving presentations on the GDPR for the last 18 months to 2 years (Appendix L).

5.2.2 Changes
This theme details both what the three employees identify as the changes needed from the GDPR as well what Bethan Bonsall from the ICO identified. The theme also included the sub-themes of “not a drastic change”, “current data protection practices” as well as “identified changes”.

5.2.2.1 Not a drastic change
Two employees within Company X referred to the change as a “20% top up”. The GDPR wishes to add the 20% to the already 80% of data protection practices that are currently in place. Bethan supported this by saying there are

“a lot of similar principle based approaches between the two laws with a few tweaks here and there” (Appendix L, lines 91-92).

She also made the point of saying that companies which already have a good grasp on data protection and understand the requirements under the Data Protection Act will find the jump a lot easier.
5.2.2.2 Current data protection practices

Throughout the interviews all three employees made various comments about the current data protection practices they have in place. All three employees stated that they have data protection training which is reviewed annually. The training is required to be completed by everyone within the business. Interviewee 2 states that the training involves

“what to do with different data, what you can do and what you can’t do” (Appendix K, line 45).

They also stated that there are organisational policies in place, as well as two interviewees stating that a lot of what is expected of employees is covered within the employee handbook. There was also mention of the HR department having restricted access to sensitive data, with interviewee 1 stating that there are “9 people in the HR team that have full access to be able to do everything” (Appendix J, lines 27-28). Interviewee 1 and 4 also mentioned that as a HR team they make sure they validate the need for the data, with interviewee 1 saying that

“we validate who is asking, are they senior enough to access that information, do we need to consider anonymising it” (Appendix J, lines 31-33).

Some of the other practices within the theme were that paper documents are scanned over to the department, emails are encrypted and that any confidential information is disposed in a confidential waste bin.

5.2.2.3 Identified Changes

This theme identified the changes that are needed to be made under the GDPR from both the employees perspective as well as the ICO. All three employees make reference to the need for updating and reviewing their policies and processes by the 25th May, Bethan Bonsall states that having

“policies and procedures in place to help demonstrate to your data subjects, demonstrate to the ICO how you’re trying to get it right” (Appendix L, lines 69-70).
There was also mentions of consent. Interviewee 1 states that

“as a HR function we just had to double check things like asking for the right level of consent with vetting, we’ve reviewed our employment contracts and policies to make sure that they were relevant, our on-boarding forms, so we tell people that we are going to do vetting every two years, have we got the right level of consent and authorisation to do that” (Appendix J, lines 95-99).

Bethan supports this by saying that a much higher standard of consent under the GDPR, consent needs to be a “positive affirmative action” such as ticking a box or verbally consenting to something (Appendix L, lines 88-99). Employees also identified that under the GDPR the data subject access request has changed, so they are required to change that process, in which interviewee 2 stated that

“at the moment we very rarely get, like DSA requests, we very very rarely get them, so I think possibly now we’ll start getting more in because it’s more of a topic of conversation people may hear about more, so that’s something that we’ll have to consider and make sure we have a process in” (Appendix K, lines 99-102).

There were also changes such as updating the learning and development to fit in with the regulation and reporting breaches. As well as these changes, a challenge the organisation is currently going through is transferring all employees to online. As the company has grown, older employees have remained on a paper file, whereas newer employees are all electronic. Interviewee 1 states that the company is more than 30 years old, with the majority of this period there only being 300 employees. During this time, the employee’s information was paper based and would be sent to a storage facility, but he states that in preparation for making sure that they have data that is relevant before GDPR comes in, they have taken the files and identified what they need to keep and what they need to get rid of. He states that “checking what data we still hold for people, is it still relevant, destroying that data that’s not, and how do we securely and future proof the way we file it” (Appendix J, lines 65-66).
5.2.3 Supporting Material
This theme covered a range of supporting materials used to help the organisation manage the changeover. It also included the sub-themes of ICO support and guidance, external support and internal support.

5.2.3.1 Internal Support
All three employees mention that there is a GDPR project team in place to manage the changeover. Interviewee 1 states that

“we’ve set up a GDPR project team with a member from each of the functions on it which was set up early in March, planned what the legislation change was going to mean to us as an organisation and then we developed a project plan out of it, with key accountabilities, and we have meetings every month to make sure that we’re developing against those accountabilities” (Appendix J, lines 121-125).

Interviewee 4 said that they do rely on the GDPR project team to send out regular communications to the site, which they do (Appendix J, lines 81-82). The GDPR project team acts as a support and guidance material which employees can use to help the change and ensure they are compliant.

5.2.3.2 ICO Guidance and Support
All three employees make reference to the ICO in some way which has helped with the change. Interviewee 1 says in the interview “I think especially for us within HR I think the ICO already gave a lot of guidance” (Appendix J, lines 84-85). He also comments about the ICO website and a guide that the ICO produced, as well as both interviewee 2 and 4 making reference to the guide. Bethan also referenced various supporting methods offered by the ICO, such as a helpline service where they would encourage organisations to get in contact before something goes wrong and help prevent it. They also have a self-assessment tool kit on their website for organisations to use, as well as conducting audits to help and guide compliance, as well as a variety of guidance on the website available.
5.2.3.3 External Support

Employees also stated some external support materials. Interviewee 4 says

“working within the HR function, we have access to quite a few external websites so we have regular updates from Xpert HR, we also have Huw James solicitors and ACAS” (Appendix M, lines 59-60).

Interviewee 1 also mentioned CIPD and LinkedIn forums, in addition to seminars from different legal providers. He also mentioned that Company X have paid for a legal counsel, who is a data expert, and the accountable executive on the GDPR project team.

5.2.4 Proactive

This theme identified that Company X and the HR department are being proactive with the change in legislation, they have put things in motion to help the changeover. As mentioned, Company X have set up a GDPR project team to help the change. The project team was set up around a year ago so the company could plan what GDPR means to the company. The project team includes a member from each function within Company X as well the legal counsel. The GDPR project team offers support to other members within the company as well as them identifying what is required of them in order to be compliant by the 25th May. The HR department have already made steps to abide by the GDPR, such as interviewee 1 stating that they have already amended their learning e-module to include the new elements of GDPR. They have also identified that in order to be compliant with the retention and purpose of information, they have employed someone to scan through all paper based copies to make them electronic. Interviewee 1 states that by doing so:

“we’ve created a process where we scan everything into this electronic document, and then we’ve saved it with a deletion date so we can just run reports on what’s needing to be deleted this month” (Appendix J, lines 67-70).

The company also have a DPO in place as well as having upskilled employees within the organisation for the GDPR. Interviewee 1 states that
“that we have some upskilled people within this organisation who are subject matter experts on GDPR, so we’ve got some people within our legal team who have gone on training. I’m the representative from the people teams who has been on it and we’ve got some key people in the operation who deal with customer data who have also gone on a course to be signed off as compliant with GDPR or a GDPR practitioner” (Appendix J, lines 103-107).

Also, all three employees have identified that they need to review their processes and policies.

5.2.5 Impact
This theme recognised the impact the introduction of the GDPR had to Company X and the HR department. The theme can be broken down into two sub-themes, cost and time.

5.2.5.1 Cost
This theme details the cost which Company X has had to pay to help the changeover in the legislation. All three employees mentioned that the HR department are trying to have all employee data as an electronic document. Interviewee 2 and 4 stated that they have hired a temporary employee to do this. Interviewee 1 states that the department have around 50 boxes of old data, with each box holding approximately 40 files and it would take an hour to go through one file. Therefore, the company would be required to pay the temp for a couple of months of work. Interviewee 1 also stated that they have a process in place now where all electronic documents have a deletion date where you can run reports to see what needs to be deleted. This system may have been introduced as a result of this, therefore cost the company money to do so. As mentioned the company also have upskilled employees to help the changeover, as well as set up a GDPR project team, with the inclusion of an external legal counsel. The company would be required to pay to train the upskilled employees, as well as a fee for the legal counsel.
5.2.5.2 Time

This theme acknowledged that the change in legislation can be time consuming. The GDPR project team requires employees to attend meetings once a month, therefore employees have set aside to time in order to attend. Interviewee 2 stated that she has had to go through a lot of contract writing regarding third parties. All employees stated there is a need to review and update processes and policies therefore that would require time in order to put the new processes and policies in place.

6.0 Discussion

The findings of the research suggest that the GDPR is simply to update the current data protection laws in place as well offer more transparency and consistency. Although there are new obligations the HR department must meet, they already have a good grasp of data protection so the changeover will be a lot easier for them to manage. The changeover is also a lot easier due to the awareness of the new regulation, as well as there being various support to help the department at Company X. However, the HR department and the company are required to give up their time as well as the resources to manage the change. Bethan Bonsall states (Appendix L, line 27) that the GDPR is to provide data protection with a 21st century approach, as well as Elizabeth Denham stating that the digital infrastructure which is in place now was unimaginable when the Data Protection Act was introduced (ico.org.uk, 2017). Both the literature and the analysis identified that the GDPR isn’t a radical change compared the current legislation, the Data Protection Act 1998. Elizabeth Denham, the UK Information Commissioner referred to the GDPR as a “step change” as well as Bethan Bonsall stating (Appendix L, lines 91-92) that there are a lot of areas which are similar, as well as both laws being similar principle based approaches with just a few tweaks here and there (ico.org.uk, 2017). This is dependent on the current data protection practices and procedures already in place within the HR department of Company X, as Bethan Bonsall stated that if “you’re getting it right now you’ll find that gap a lot easier to navigate” (Appendix L, lines 103-104).
The findings from the data collection identified that the HR department already have various processes and procedures in place to protect their employee data ranging from policies, procedures and e-learning, therefore this would support the ideology that the HR department will find the process of change much easier compared to a company with minimal procedures and processes in place.

The findings also showed that the implementation of the GDPR hasn’t come as a surprise. Bethan Bonsall stated that the ICO have had their 12-step guide on their websites for around 2 years now as well as herself going out and giving presentations about the topic for the last 18 months to 2 years. Employees were also aware of the change, with them all stating that it was at least a year ago they were aware of the regulation. A huge factor of the awareness of the GDPR is down to the huge increased fines, which Bethan Bonsall states “really do reflect the importance of personal data” (Appendix L, lines 165-166). The ICO state that they will always prefer the approach of engagement over enforcement and will only issue fines as a last resort, however these increased fines act as a huge deterrent to organisations. The literature review shows the much higher ramifications if an organisation fails to comply with the GDPR compared to the Data Protection Act. Bethan Bonsall states (Appendix L, line 19) that organisations are interested more than ever in getting data protection right, a huge factor in this will most likely be the increased fines as they have much more of an impact.

The changes that the department would need to be aware of which were mentioned within the literature review were also detailed within the results. The department identified the new accountability principle as well as needing to review their lawful basis for processing. The results identified that the department already had a lot of processes and procedures in place so the overall consensus was that they just needed to review their policies and procedures and ensure that they are compliant by May 25th. The department had already started to implement changes to come in align with the GDPR by creating a GDPR project team, consisting of members from each function as well as support from a legal counsel. This is supported by the findings in the literature that there is a need for an organisation to create a compliance programme, with DLA Piper stating that a feature of the implementation is to assemble a project team, which leads on to assessing potential areas of exposure in current working processes, create a plan of action to be compliant, implement changes and finally establish a governance framework to manage risk (Dlapiperbeaware.co.uk, 2018).
The department also hired a temporary member of staff to scan all paper files onto an electronic document so that they could identify what data was needed and what needed to be deleted, this also included a deletion report that could be generated due to all files now being electronic.

As well as the department having identified the changes needed to be made and having started to be proactive with the changeover, the results found that they have a huge range of supporting materials that can be used to ease the process. Internally they have the GDPR project team, which the results showed would meet and identify changes and how they need to tackle them and filter that information down through the department. Externally, they have access to websites such as CIPD, XpertHR, ACAS and the ICO. Bethan Bonsall from the ICO details various supporting materials on their website such as a self-assessment tool as well sector specific advice. In addition to having material on their website she also stated that they have a helpline, audits and presentations on the GDPR (Appendix L).

The findings did identify that although there was a big awareness of the change in the legislation, as well the department itself identifying changes and being proactive with them, including various methods of support and guidance towards the change, the changeover does require time and resources. As previously stated, the process of going back through policies, processes and contracts requires time. Also, the GDPR project team members are required to give up their time to attend meetings. Not only is time required, but for the department to be compliant it requires the company to invest in resources. The company appointed a DPO, which would be at a labour cost to the company. They also took on a temporary member of staff to scan all paper files, which again would be at a cost. Additionally, the organisation paid for an external legal counsel to help with the process.

The findings from the research suggests that the HR department are on track to be compliant with the GDPR by May 25th, 2018. They are being proactive with the change and have already identified changes that, as a department, they need to make. Bethan Bonsall states that the principles are a framework for an organisation to work with, giving an example that the requirements of a small corner shop in Cardiff would be entirely different compared to Cardiff Council (Appendix L, lines 58-62). Organisations are required to apply themselves to the principles, which is what the department are looking to do.
The increased fines reflect the importance of protection of personal data and act as a huge deterrent and focuses organisations on the importance of data protection. The department have various supporting materials available as well strong processes and procedures already in place, therefore only small changes are required. Although these are small changes, it requires the organisation to put time and money into the process to ensure compliance.

The research only looked at one case study with all findings linking directly to a specific company and that HR department experiences. This was to achieve in-depth research and investigate the impact the GDPR has on one specific company, as well working within a restricted timescale. Therefore, the findings for another HR department in a different company could be completely different. Further research could look at smaller organisations that may not have the external support such as CIPD, XpertHR, or the resources and time to create a GDPR project team and hire more staff to deal with the changeover.

7.0 Conclusion

The GDPR has been introduced to update the main current data protection law, the Data Protection Act 1998. Company X and the HR departments current practice of data protection requires them to comply with all eight principles under the Act, however, as of the 25th May 2018 there will be new obligations that the department and company must comply with. The research looked to identify current practices and identify the changes the department would need to be aware of and the impact this would generate. The literature review looked to identify the changes under the GDPR that will directly affect the department and what they will need to do in order to be compliant. It also detailed the increased ramifications under the GDPR in comparison to the Data Protection Act, with one relevant case study.

The analysis supported the literature review as the department looked to address the same changes which were highlighted. The results identified that the GDPR changes are simply a small change if the organisation has a strong foundation of data protection already in place, therefore the changes in legislation for the department and company were only minor. However, the department has several supporting materials in place to assist with the change, ranging from an internal GDPR project team to a variety of websites, such as ACAS and CIPD. Furthermore, the ICO offer their own guidance and support. The main impact towards the department and the company is that the new implementation of the GDPR required both
time and money. Although this required upfront resources in order to be compliant, this would benefit the organisation in the long run as it would prevent them from receiving substantial fines under the GDPR for non-compliance.

The research identified that the HR department is most likely to be compliant by the 25th May 2018, due to them having a solid foundation of data protection. In addition to this, the awareness of the GDPR itself gave them sufficient time to be compliant. They also had access to various supporting materials and resources to aid the changes. However, this might not be the same for a smaller organisation with less access to supporting material, as well as a much tighter restraint on resources. The GDPR can affect organisations in entirely different ways depending on numerous factors. Therefore, in order to be compliant, it is vital that an organisation looks to apply themselves to the principles and use tools and techniques to identify key aspects of their data protection and put together a plan to address concerns.

For organisations that may be struggling with the implementation of the GDPR, and worrying due to the mention of the increased fines that can be imposed, there is support and guidance available. The ICO offers a wide range of support and tools for organisations, and issuing fines is seen as a last resort scenario, with the main priority of the ICO being engagement over enforcement. The implementation of the new regulation is not to catch organisations out, but to simply adapt data protection laws to this technological era and for people to be able to trust organisations with their data and to try and reduce the frequency and quantity of data breaches.
8.0 References


Press Association, 2016. Council fined £100,000 after social care files left in empty building. The Guardian, 17 August


Stibbs, N. (2018). Data Protection. [online] Available at: https://www.xperthr.co.uk/employment-law-manual/data-
protection/20363/?keywords=failure+to+comply+with+the+data+protection+act+1998 [Accessed 6 Feb. 2018].


### 9.0 Appendices

**Appendix A – Ethics Form**

**Approved Ethics Number - 2016D5736**

<table>
<thead>
<tr>
<th>Name of applicant:</th>
<th>Gerard Counsell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor (if student project):</td>
<td>Taslima Begum</td>
</tr>
<tr>
<td>School / Unit:</td>
<td>Cardiff School of Management</td>
</tr>
<tr>
<td>Student number (if applicable):</td>
<td>ST20072673</td>
</tr>
<tr>
<td>Programme enrolled on (if applicable):</td>
<td>BSc (Hons) Business Information Systems</td>
</tr>
<tr>
<td>Project Title:</td>
<td>An investigation into how a HR department within a Cardiff based company deal with changes of the Data Protection Act to the new General Data Protection Regulation</td>
</tr>
<tr>
<td>Expected start date of data collection:</td>
<td>15/01/2018</td>
</tr>
<tr>
<td>Approximate duration of data collection:</td>
<td>6-8 Weeks</td>
</tr>
<tr>
<td>Funding Body (if applicable):</td>
<td>N/A</td>
</tr>
<tr>
<td>Other researcher(s) working on the project:</td>
<td>N/A</td>
</tr>
<tr>
<td>Will the study involve NHS patients or staff?</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve human samples and/or human cell lines?</td>
<td>No</td>
</tr>
</tbody>
</table>

**Does your project fall entirely within one of the following categories:**

- Paper based, involving only documents in the public domain: No
- Laboratory based, not involving human participants or human samples: No
- Practice based not involving human participants (eg curatorial, practice audit): No
- Compulsory projects in professional practice (eg Initial Teacher Education): No
- A project for which external approval has been obtained (e.g., NHS): No

If you have answered YES to any of these questions, expand on your answer in the non-technical summary. No further information regarding your project is required.

If you have answered NO to all of these questions, you must complete Part 2 of this form.
In no more than 150 words, give a non-technical summary of the project

To conduct a feasibility study into identifying the key changes of legislation from the Data Protection Act 1998 to the General Data Protection Regulation 2018. The study will look at a HR department within a Cardiff based company and how they abide by these legislations and the changes they will need to take in order to stay in line with current data protection law. The study will also look at the possible ramifications if the company were to break any conditions of the legislation. The study will entail the use of both primary and secondary research for the researcher to get the most information available for the study.

DECLARATION:
I confirm that this project conforms with the Cardiff Met Research Governance Framework

I confirm that I will abide by the Cardiff Met requirements regarding confidentiality and anonymity when conducting this project.

STUDENTS: I confirm that I will not disclose any information about this project without the prior approval of my supervisor.

<table>
<thead>
<tr>
<th>Signature of the applicant:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gerard Counsell</td>
<td>14th December</td>
</tr>
</tbody>
</table>

FOR STUDENT PROJECTS ONLY

<table>
<thead>
<tr>
<th>Name of supervisor:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taslima Begum</td>
<td>14th December</td>
</tr>
</tbody>
</table>

| Signature of supervisor: | |
|--------------------------| |
| Taslima Begum            | |

Research Ethics Committee use only

| Decision reached: | |
|-------------------| |
| Project approved  | |
| Project approved in principle | |
| Decision deferred | |
| Project not approved | |
| Project rejected  | |

Project reference number: Click here to enter text.

Name: Click here to enter text. | Date: Click here to enter a date.

Signature:

Details of any conditions upon which approval is dependant:
## PART TWO

### A RESEARCH DESIGN

<table>
<thead>
<tr>
<th>A1 Will you be using an approved protocol in your project?</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 If yes, please state the name and code of the approved protocol to be used</td>
<td>N/A</td>
</tr>
<tr>
<td>A3 Describe the research design to be used in your project</td>
<td>The study will utilise a mono method, which consists of just using one qualitative or quantitative research. Due to nature of the study the method of qualitative research using interviews only is the best way to gain information directly about the company and how they will deal with the legislations as well as to find out the possible ramifications if not met. Interview – I will aim to find participants for the interviews, selecting participants based on their role within the company and also look at some participants outside of the company but based on their role and the industry they’re in. Therefore, the sampling method used for the interviews would be Non-Probability Sampling. The interviews will be either face to face or over the telephone. The questions for the interviews would follow a semi-structure format which consists of using themes or key questions to ask the interviewee. The study would look at 3-4 initial interviews in the hope to get all the information needed for the study but may require an extra 1-2 if needed. For the interviews, an information sheet will be given to the participants outlining the aim and objectives of the study, which would then be followed by a consent form to be signed by the participant. All the participant’s which work for the company which the study is based on with remain anonymous due to not wanting to expose their company but the participant’s outside the company will be known. All participants are given the opportunity to withdraw within 7 days of completing the interview.</td>
</tr>
<tr>
<td>A4 Will the project involve deceptive or covert research?</td>
<td>No</td>
</tr>
<tr>
<td>A5 If yes, give a rationale for the use of deceptive or covert research</td>
<td>Non applicable</td>
</tr>
<tr>
<td>A6 Will the project have security sensitive implications?</td>
<td>No</td>
</tr>
<tr>
<td>A7 If yes, please explain what they are and the measures that are proposed to address them</td>
<td>Non applicable</td>
</tr>
</tbody>
</table>
### B Previous Experience

**B1** What previous experience of research involving human participants relevant to this project do you have?

Some experience in conducting primary research through the use of interviews. This research was obtained through the module of “E-business Management BCO5021” by interviewing a business owner about their e-business infrastructure.

**B2 Student project only**

What previous experience of research involving human participants relevant to this project does your supervisor have?

Taslima Begum has had 10+ years’ experience

### C Potential Risks

**C1** What potential risks do you foresee?

Interviews can be risky due to the participants not wanting to take time out of their day to attend an interview. Another risk is the interview process taking a large amount of time and putting the study at risk.

Another risk is related to the participants themselves, as they are placing their trust in the process, ensuring that their information from the interviews is kept secure and anonymous, and the information gathered is kept for the study and not passed on to any third parties. In addition to this the results from the interviews may not be accurate depending on the honesty of participants.

Another issue is the planning and process of the study, with the risk of falling behind with deadlines or parts of the study. This can put the project at risk and possibly affect the outcome or the study being incomplete.

**C2** How will you deal with the potential risks?

I will organise interviews early on, ensuring time for them to be completed. To do so, I will have a list of several people I can contact for the interviews. To protect participants and ensure there are no doubts regarding security or remaining anonymous, each participant will be given an information sheet containing details of the study and the aim and objectives, followed by a consent form to be signed. I will look to keep up to date and in contact with my supervisor throughout the study to ensure the completed project is on track.
PARTICIPANT INFORMATION SHEET

Key changes to the General Data Protection Regulation 2018 from the Data Protection Act 1998 and how these impact a HR department

Project summary
The purpose of this research project is to identify the changes of data protection legislations and how they will impact a HR department and how the department adapt to these changes. Your participation will enable the collection of data will form part of a study undertaken at Cardiff Metropolitan University.

Why have you been asked to participate?
You have been asked to participate due to your role within the company that is under study. During the interview, you will be asked about your role within the company and the impact of the changing legislation and how as a department you've dealt with that. Your participation is entirely voluntary and you may withdraw at any time.

Project risks
The research involves the participation in an interview which will be recorded for later analysis. We are not seeking to collect any sensitive data on you; this study will look at how the department deals with the changes and the impact the legislation change has had. We do not think that there are any significant risks associated with this study. However, if you do feel that any of the questions are inappropriate then you can stop at any time. Furthermore, you can change your mind and withdraw from the study at any time and the decision will be completely respected.

How we protect your privacy
All the information you provide will be held in confidence. Careful steps have been taken to make sure that you cannot be directly identified from the information given by you. Your personal details such as your signature on the consent form will be kept in a secure location. When the study is completed and all the information is analysed, the documentation used to gather the data will be destroyed apart from your signed consent form which will be held securely for 5 years. The recordings of the interview will also be held in a secure and confidential environment during the study and destroyed after 5 years.

YOU WILL BE OFFERED A COPY OF THIS INFORMATION SHEET TO KEEP

If you require any further information about this project then please contact:
Gerard Counsell, Cardiff Metropolitan University
Cardiff Metropolitan University email: st20072673@outlook.cardiffmet.ac.uk
PARTICIPANT INFORMATION SHEET

Key changes to the General Data Protection Regulation 2018 from the Data Protection Act 1998 and how these impact a HR department

Project summary
The purpose of this research project is to identify the changes of data protection legislations and how they will impact a HR department and how the department adapt to these changes. Your participation will enable the collection of data will form part of a study undertaken at Cardiff Metropolitan University.

Why have you been asked to participate?
You have been asked to participate due to your role within the data protection industry. During the interview, you will be asked about your role within your organisation and the key changes of the legislations and the possible ramifications if companies do not comply with them. Your participation is entirely voluntary and you may withdraw at any time.

Project risks
The research involves the participation in an interview which will be recorded for later analysis. We are not seeking to collect any sensitive data on you; this study will look at how the department deals with the changes and the impact the legislation change has had. We do not think that there are any significant risks associated with this study. However, if you do feel that any of the questions are inappropriate then you can stop at any time. Furthermore, you can change your mind and withdraw from the study at any time and the decision will be completely respected.

How we protect your privacy
All the information you provide will be held in confidence. Careful steps have been taken to make sure that you cannot be directly identified from the information given by you. Your personal details such as your signature on the consent form will be kept in a secure location. When the study is completed and all the information is analysed, the documentation used to gather the data will be destroyed apart from your signed consent form which will be held securely for 5 years. The recordings of the interview will also be held in a secure and confidential environment during the study and destroyed after 5 years.

YOU WILL BE OFFERED A COPY OF THIS INFORMATION SHEET TO KEEP

If you require any further information about this project then please contact:
Gerard Counsell, Cardiff Metropolitan University
Cardiff Metropolitan University email: st20072673@outlook.cardiffmet.ac.uk
Appendix D – Consent form Interviewee 1

Cardiff Metropolitan University
Ethics Committee

PARTICIPANT CONSENT FORM

Participant name: [Redacted]
Title of Project: An investigation into how a HR department within a Cardiff based company will deal with the changes of the Data Protection Act to the new EU’s General Data Protection Regulation.
Name of Researcher: Gerard Counsell

Participant to complete this section: Please initial each box.

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. [ ]

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason. [ ]

3. I agree to take part in the above study. [ ]

4. I agree to the interview being recorded [ ]

5. I agree to the use of anonymised quotes in publications [ ] [ ]

6. I would like my organisations’ name to be anonymised in all publications [ ] [ ]

Signature of Participant ______________________________ Date __________
Name of person taking consent ______________________________ Date __________
Signature of person taking consent ______________________________
Appendix E – Consent form Interviewee 2

Cardiff Metropolitan University
Ethics Committee

PARTICIPANT CONSENT FORM

Participant name: [Redacted]
Title of Project: An investigation into how a HR department within a Cardiff based company will deal with the changes of the Data Protection Act to the new EU’s General Data Protection Regulation.
Name of Researcher: Gerard Counsell

Participant to complete this section: Please initial each box.

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. [ ]

2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason. [ ]

3. I agree to take part in the above study. [ ]

4. I agree to the interview being recorded [ ]

5. I agree to the use of anonymised quotes in publications
   Yes [ ] No [ ]

6. I would like my organisation’s name to be anonymised in all publications [ ]

[Redacted]

Signature of Participant Date 13/03/2018

Gerard Counsell

Name of person taking consent Date 13/3/18

[Redacted]

Signature of person taking consent
Appendix F – Consent form Interviewee 3

Cardiff Metropolitan University
Ethics Committee

PARTICIPANT CONSENT FORM

Participant name:
Title of Project: An investigation into how a HR department within a Cardiff based company will deal with the changes of the Data Protection Act to the new EU’s General Data Protection Regulation.
Name of Researcher: Gerard Counsell

Participant to complete this section: Please initial each box.

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. [ ]

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason. [ ]

3. I agree to take part in the above study. [ ]

4. I agree to the interview being recorded [ ]

5. I agree to my quotes being attributed to me Yes No [ ]

6. I agree to my organisation being named in all publications [ ]

Signature of Participant 19/3/18
Date
Name of person taking consent 19/3/18
Date
Signature of person taking consent
Appendix G – Consent Form Interviewee 4

Cardiff Metropolitan University
Ethics Committee

PARTICIPANT CONSENT FORM

Participant name: [Redacted]
Title of Project: An investigation into how a HR department within a Cardiff based company will deal with the changes of the Data Protection Act to the new EU's General Data Protection Regulation.
Name of Researcher: Gerard Counsell

Participant to complete this section: Please initial each box.

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. [x]

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason. [x]

3. I agree to take part in the above study. [x]

4. I agree to the interview being recorded [x]

5. I agree to the use of anonymised quotes in publications [x] [ ]

6. I would like my organisations’ name to be anonymised in all publications [x] [ ]

Signature of Participant: [Redacted] Date: 2/4/18
Name of person taking consent: [Redacted] Date: 2/4/18
Signature of person taking consent: [Redacted]
### Appendix H – Company X Semi Structured Interview Questions

<table>
<thead>
<tr>
<th>Order of semi structured interview</th>
<th>Discussed</th>
</tr>
</thead>
</table>
| 1) Ask respondent approval to use recording systems  
Ask respondent to sign and acknowledge consent form |                |
| 2) Ask background questions  
Confirm questions about;  
* Respondents position  
* Number of years working for the organisation |                   |
| 3) **Discuss current data protection procedures**  
Probes  
* What employee data do you hold?  
* How do ensure the safety / security of employee data?  
* What data protection policies do you currently have in place?  
* Have you had training? If yes when and is there annual review?  
* What is the biggest challenge right now with data protection in your department? |                         |
| 4) **Discuss General Data Protection Regulation**  
Probes  
* When did you first hear about the change in legislation?  
* What did you identify as key changes of legislation?  
* How has the department dealt with these changes?  
* Did you use any techniques/tools or materials to help support the change to the new legislation?  
* How have these changes impacted the department? |                  |
| 5) **Discuss Ramifications of General Data Protection Regulation**  
Probes  
* Are you aware of the possible outcomes against the company if a breach of legislation occurs?  
* Are you and other employees aware that you can be subject to liability personally for failure to comply and direct action can be taken by regulators, controllers and data subjects?  
* How do you ensure you fully comply with the new legislation in practice? |                      |
### Appendix I - ICO Semi Structured Interview Questions

<table>
<thead>
<tr>
<th>Order of semi structured interview</th>
<th>Discussed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Ask respondent approval to use recording systems&lt;br&gt;Ask respondent to sign and acknowledge consent form</td>
<td></td>
</tr>
<tr>
<td>2) Ask background questions&lt;br&gt;Confirm questions about;</td>
<td></td>
</tr>
<tr>
<td>• Name of the organisation</td>
<td></td>
</tr>
<tr>
<td>• Respondent's position</td>
<td></td>
</tr>
<tr>
<td>• Number of years working for the organisation</td>
<td></td>
</tr>
<tr>
<td>3) Discuss the General Data Protection Regulation&lt;br&gt;Probes</td>
<td></td>
</tr>
<tr>
<td>• Why was the General Data Protection Regulation introduced?</td>
<td></td>
</tr>
<tr>
<td>• What does it hope to achieve?</td>
<td></td>
</tr>
<tr>
<td>• What are the main changes from the Data Protection Act to the General Data Protection Regulation?</td>
<td></td>
</tr>
<tr>
<td>• What do you think are the key challenges companies will face in terms of updating their compliance?</td>
<td></td>
</tr>
<tr>
<td>• What support or materials are out there to help companies comply with the new legislation?</td>
<td></td>
</tr>
<tr>
<td>4) Discuss the failure to comply within the General Data Protection Regulation</td>
<td></td>
</tr>
<tr>
<td>• What are the ramifications if a company doesn't comply with the General Data Protection Regulation?</td>
<td></td>
</tr>
<tr>
<td>• Why were the ramifications altered from the previous Data Protection Act?</td>
<td></td>
</tr>
<tr>
<td>5) Discuss the future of the General Data Protection Regulation</td>
<td></td>
</tr>
<tr>
<td>• Do you think all companies will be fully compliant by the 25th May?</td>
<td></td>
</tr>
<tr>
<td>• What will happen to the General Data Protection Act when the UK exit the EU?</td>
<td></td>
</tr>
<tr>
<td>• What is the future for data protection within the UK?</td>
<td></td>
</tr>
</tbody>
</table>
Appendix J – Transcript from Interview 1

Interviewer: Alright are you ready?

Interviewee 1: Yeah

Interviewer: So, the first is just to ask for approval to the use of recording?

Interviewee 1: Yes, that’s fine I’m happy to

Interviewer: The consent form, you’ve signed and acknowledged it?

Interviewee 1: Yeah

Interviewer: And then just background questions, um so what is your position within the company?

Interviewee 1: I am the HR Manager that looks after the day to day HR operations and I am an HR business partner

Interviewer: Ok brilliant, and how long have you been doing that?

Interviewee 1: I’ve been here for a year and was at a utility company for 10 years before that

Interviewer: Ok brilliant. So, this is about the current data protection procedures in regard to the data protection act. So, the first one is what employee data do you hold?

Interviewee 1: We hold a range of sensitive and less sensitive data, so we collect everything from what you’d expect, name and address, bank details, we collect information around gender, sexual orientation, race, ethnic origin, and a huge amount more

Interviewer: Ok

Interviewee 1: Do you want me to try and list everything out for you?

Interviewer: not everything, as long as, just a difference between sensitive and less sensitive, so there’s obviously different categories for the two, for the legislation so that’s fine as long as there’s both that’s fine. How do you ensure the safety and security of employee data?

Interviewee 1: We have a few means of doing that. One is that only people within the HR function get to access a lot of data, especially the sensitive stuff, such as the bank details and stuff like that. We run the payroll book and process that ourselves, we don’t share that data
with anyone else. That is only available through accessing our system and through having authorised access, so there is only 9 people in the HR team that have full access to be able to do everything, and then the other step is sometimes from time to time we’re asked for reports from the operations, so can I have a report that tells me this amount of information, for example I want sickness information for everyone in the team, we just have to check that they have a need for that data, that is relevant, and not just willy nilly asking for stuff. So, we validate who is asking, are they senior enough to access that information, do we need to consider anonymising it, sometimes the bid team ask for length of service reports for example, but then that’s confidential information, so you don’t want to just give out as a HR function data unnecessarily so we just validate is it absolutely necessary for what they need and is there any way we could give it to them anonymised?

**Interviewer:** Ok brilliant. what data protection policies do you currently have in place?

**Interviewee 1:** as a HR team or as an organisation?

**Interviewer:** Organisation.

**Interviewee 1:** We have a few, so we have data retention policies, because we have different data points for different things, so we have a HR schedule within that, for example customer schedule, marketing schedule. We have a data protection policy which is more general as well, we have a data protection E-Learning module, and we have a data subject access request policy, which maps out how exactly we will process, if we get a d cell request, exactly how we process that.

**Interviewer:** Ok brilliant. You kind of answered this one, but with regards to the training, so I’m assuming that’s the E-Learning module that they do for staff? So that’s a yes, but is there an annual review? Like how often do they complete that?

**Interviewee 1:** So, whenever anyone is inducted face to face they have a three-day induction and data protection is covered off there, and already we’ve updated that to cover off some of the new elements of GDPR and once they’ve done the three-day induction they do about an hour-long E-Learning module around data protection and then that is renewed annually then.
Interviewer: Ok brilliant. What is your biggest challenge right now with data protection within
the HR department?

Interviewee 1: I think our biggest challenge has been that, this company is more than 30 years
old, and for a long time it was very small and only employed 300ish people, and what we have
done historically is had paper files for everyone, put everything in those paper files and then
when that colleague would leave we would send it to a storage facility, like Maltings or Crown,
so in preparation for making sure that have we got data that’s relevant before GDPR comes
in, and we probably should have been doing it anyway, but I only found out a few months ago
that we had about 50 boxes of old data, so our challenge has been, and say each box holds
maybe 40 files, and a file takes about an hour to look through and process and decide what
do we need to keep and what do we not, so our challenge has been our book keeping I
suppose, our administration of checking what data we still hold for people, is it still relevant,
destroying that data that’s not, and how do we securely and future proof the way we file it,
so we’ve created a process where we scan everything into this electronic document, and then
create, we’ve saved it with a deletion date so we can just run reports on what’s needing to
be deleted this month, so our biggest challenge has been dealing with this massive load of
data files.

Interviewer: Ok brilliant. So, this is regarding the GDPR, so when did you first hear about the
change in legislation?

Interviewee 1: Good question. When I first started here we were already talking about it a
year ago, so last march and I don’t know. I remember then specifically, but I can’t remember
anything before then. I remember reading articles about it, remember getting marketing
e-mails from HR businesses trying to sell it quite quickly and then we have a platform called
XpertHR, which has a catalogue of all the legislation changes that are coming up and I
remember when it was first announced we were twooting and throwing about whether because
of Brexit whether we would have to actually do it or not because we might exit before it
comes regulation and what, and it was decided that we definitely are doing it. That could have
been 18 months ago, two years ago, I can’t remember specifically.

Interviewer: Yeah that’s fine. So, in terms of the GDPR what did you identify as the key
changes from there to the data protection act?
Interviewee 1: I think especially for us within HR I think the ICO already gave a lot of guidance and they have a guide called the employers practice guide I think which covers an awful lot of stuff and when we met with the ICO to explore what were the main things and what do we need to do differently, they said the thing to remember is that data protection and the data protection act covers already about 80% of what we do and what GDPR does is top that up by 20%, it doesn’t, it’s not a radical overhaul of data protection law, it’s just a small change, so the main things we identified that we need to do differently, as an organisation, think about how we’re asking for consent with marketing, because we manage customer data, like because we develop software for banks for example, and then we hold their customer data on that software, we needed to make sure that we were compliant but then also make sure that on the other side of that they were being compliant with GDPR regulation too, so we had to attest that somehow. And then as a HR function we just had to double check things like asking for the right level of consent with vetting, we’ve reviewed our employment contracts and policies to make sure that they were relevant, our on-boarding forms so we tell people that we are going to do vetting every two years, have we got the right level of consent and authorisation to do that, so do we have legitimate interests or not, and then do we have a correct DSAR process in places is still up to date, so looking at all other policies and making sure it’s still going to be relevant in May, and then the other thing, because we within HR we look after the learning and development function as well, it’s making sure that our modules are updated for our e learning going forward and that we have some upskilled people within this organisation who are subject matter experts on GDPR, so we’ve got some people within our legal team who have gone on training, I’m the representative from the people teams been on it and we’ve got some key people in the operation who deal with customer data who have also gone on a course to be signed off as compliant with GDPR or a GDPR practitioner.

Interviewer: Brilliant. You kind of already mentioned, so in terms of, it just talks about how the department deal with the changes so that’s fine. In terms of dealing with these changes you mentioned expert HR and the ICO talking to you, were there any other techniques or tools or materials to support the change?

Interviewee 1: Yes, I think there’s lots of documents that have been flying around, different templates for how to carry out a data audit within the company, how to prepare yourself from a HR point of view, so CIPD have released some papers, every now and then, I’m in a
few forums on linked in and every now and then people have shared documents that they
found useful within those forums, so it’s just looking at those two. Whenever I’ve attended
seminars, and I’ve gone to a few from different legal providers, they almost always give you
a pack of things that are useful to know, so I’ve got like a little bible of bits and bobs to look
at. And jumping back a step, you asked about how we prepare?

Interviewer: How have they dealt with the changes?

Interviewee 1: Yeah, I think just to pull out that we, as an organisation, we’ve set up a GDPR
project team with a member from each of the functions on it which was set up early in March,
planned what the legislation change was going to mean to us as an organisation and then we
developed a project plan out of it, with key accountabilities, and we have meetings every
month to make sure that we’re developing against those accountabilities.

Interviewer: Ok brilliant. So, the last one was how have these changes impacted the
department?

Interviewee 1: I think we, I think for us, I think sometimes data protection can fall off the
radar as being important, I think it’s pulled it back into our radar a little bit more and made
people more conscious of am I doing the right thing, am I making sure that I’m not leaving
any sensitive data out, am I making sure that I’m stood by the printer when I’m printing stuff
out, am I being compliant with the current data protection act, but then also it’s checking the
whole team to make sure they’re aware of the changes. And I think that’s it.

Interviewer: Ok brilliant. The last one is just the ramifications under the data protection act.
So the first one is are you aware of the possible outcomes against the company if breach of
legislation occurs?

Interviewee 1: So, it varies anything from having, you can be written to and told this is what’s
gone wrong, this is remediation. Under data protection act there was the ICO, had a right to
investigate and enforce a fine, with GDPR it’s exactly the same process accept the ability to
fine has gone up, no the value of the fine has gone up.

Interviewer: Yeah that’s fine. Are you and other employees aware that you can be subject to
liability personally for failure to comply and direct action can be taken by regulators,
controllers and data subjects?
Interviewee 1: Yes, we are under a certain set of, like it wouldn’t jump to an individual being blamed for the whole organisation necessarily, but we have a DPO, they are liable for making sure that we’re complying with the GDPR, so that person would be, if something happened that was an accident, that person necessarily wouldn’t be automatically liable, if they did something carelessly, potentially or frequently they could be personally liable.

Interviewer: Yeah, but I think in terms of personally that now under the GDPR, a data processor can be subject to a fine under the data subject.

Interviewee 1: Yeah

Interviewer: Yeah, that’s fine. And then the last one was just kind of probably what you’ve kind of already talked about, but how do you ensure you are fully compliant with the new legislation?

Interviewee 1: I think it’s through making sure that we have attended legal seminars and paid for some consultancy about what we should be doing and is everything that we’re doing going down the right track. We’ve got an internal legal team that are a commercial legal team, and we employed a senior legal counsel who is a data protection expert, whose been the accountable exec on the project here, and they’ve been keeping up to date with lots of documentation that’s come out since, because there’s so much information on the ICO website and other websites about definitions and like, legislation can be quite complex and hard to guide yourself through, so we’ve employed a senior legal counsel who can help give us guidance on what exactly it should mean for us as an organisation and what are other people doing out there. So, yeah, using those, using the project group, checking in with different legal advisors, checking in with the ICO from time to time about stuff and reading blogs and information from independent commissioners and policy writers just to check what they’re guidance is or what questions they’re being asked and what they’re doing with it, so as an organisation we’re staying up to date.
Appendix K – Transcript from Interview 2

Interviewer: Ok so the first, is just the approval of me recording?

Interviewee 2: Yeah

Interviewer: That’s fine. And the second one is just about the consent form and that you’ve acknowledged it?

Interviewee 2: Yeah

Interviewer: Ok. It starts off with just background questions, so what is your position within the company?

Interviewee 2: I’m a HR advisor at Company X

Interviewer: What exactly does that entail?

Interviewee 2: So, my role specifically, I look after a mass media company who’s a new project that’s coming in and then I also help out, I support servicing for employee relations cases and support on any new bids coming in, so the time and organisational changes, things like consultancies and TUPE (Transfer of undertakings) and stuff I’ll do the data in the background for the preparation.

Interviewer: How long have you been doing that for?

Interviewee 2: So, I’ve been a HR advisor in Company X since December last year. Before that, I was a HR coordinator, which was quite a similar role I just wasn’t doing as much employee relations things, and then I was HR coordinator for about 10 months and then before that I was HR administrator which was kind of more of the just inputting data and stuff like that.

Interviewer: Ok, the next one is just on the current data protection procedures. So, the first one is just what employee data do you hold, in terms of just a couple of different examples?

Interviewee 2: So, in terms of like bank details and things like that?

Interviewer: Yeah

Interviewee 2: So, when people join the company we ask them to complete a new starter welcome pack, that ranges from there a quite a few different forms in there, there’s an equal opportunity form which contains things about their background, disabilities, if they have
children, things like that. Then, group life insurance form, which is who they would nominate
to receive any money if they died while working at Company X, new starter advice form which
has got their next of kin, emergency details, bank details, their NI number, all of that. I think
that’s it.

**Interviewer:** Yeah that’s fine. So how do you ensure the safety and security of employee data?

**Interviewee 2:** So, any documents that, paper documents we ask people to scan it over to us,
and if they give us a paper version we dispose of it in the confidential waste bin straight away.
If I’m emailing, so for instance, an occupational health request or something like that which
contains information about somebody’s absences or anything like that I’ll always send it so
its protected, so ill encrypt the document before I send it over. So yeah, things like that.

**Interviewer:** Ok that’s fine. What data protection policies do you currently have in place?

**Interviewee 2:** We do have one but it’s not very, I think, it’s kind of more implied, like people
just do things because they know that you can’t leave data or documents out, just kind of in
the middle of some..

**Interviewer:** So would that be in an employee handbook kind of thing?

**Interviewee 2:** Yeah exactly that, yeah

**Interviewer:** So is there a training for data protection?

**Interviewee 2:** Yeah, so you receive E-Learning training on the data protection and kind of,
what to do with different data, what you can do, what you can’t do. If you don’t pass that
module, you have another chance to do it, but if not then it gets escalated to your line
manager to do and everyone in the business does that.

**Interviewer:** Is that annually, or like?

**Interviewee 2:** I’ve got a feeling its twice a year actually but I can check for you with the
learning development team.

**Interviewer:** Yeah that’s fine. What is your biggest challenge right now with data protection
in your department?
Interviewee 2: Because we do have access to so much employee information, I’d say, and it’s all kind of, they’re all documents kind of on the system, potentially somebody, you could delete a document without even realising, stuff like that, and it’s on there, or save a document in the incorrect person’s file. I don’t find that, because we’re trying to go paperless, we don’t have documents lying around in the same way, I do think we are getting better now at disposing of information after kind of the 7 years, whereas, but again, there are certain documents because we’re HR that we need to keep hold of just for information record keeping purposes. So yeah, it’s just working out what is acceptable and not acceptable to keep.

Interviewer: Ok brilliant. So, the next bits just about the GDPR. When did you first hear about the change in legislation?

Interviewee 2: Probably first heard about it when, a few months before we kicked off the project at Company X, which was about, probably a year ago we kicked off the project. I heard about it and I knew we kind of had to do changes, but id spoken to Interviewee 1 about it who’d assured me that as, because of the way we already work, it’s not going to affect us massively in the same way it would affect marketing and things like that, so it’s just us getting stricter with things like that, yeah.

Interviewer: Ok, the next one is what did you identify as the key changes of the legislation?

Interviewee 2: So, identifying that people obviously don’t have to pay the £10 if they want any information anymore, they, I guess from my point of view maybe not a HR point of view, in terms of, you can, the right to be forgotten, the change of, like you can compare lists now, like if you have data, if you do a shopping list on one website you can compare it and just bring it over because they can’t just keep that data on one particular website and stuff like that.

Interviewer: Ok brill. The next one is how has the department dealt with the changes?

Interviewee 2: So Interviewee 1 has worked very closely with the GDPR project team and then I have sat down with a few of the project managers and looked at all of the different third parties, so I’ve been looking at the third party companies that we deal with specifically and how they use our data, what they use our data for and whether their GDPR client, sorry,
GDPR compliant themselves so we’re currently going through that so that’s a lot of contract writing for my part in like checking what they do. I think we are, we are, we’ve currently got somebody going through all of our files at the moment, scanning stuff on and disposing of any data that’s over 7 years old isn’t needed.

**Interviewer:** Ok brill. Did you use any techniques or tools and materials to kind of help support the change to the new legislation?

**Interviewee 2:** I have looked at the GDPR guidelines, both the employee and the employer’s guidelines.

**Interviewer:** Is that the ICO?

**Interviewee 2:** Yeah. I think they are good, but only if you have a basic understanding of GDPR already. So, but, yeah, I’ve kind of looked at that, but we’ve had a lot of support because it’s been such a big project, the biggest project I think Company X have done in terms of technology, we’ve had a lot of support and advice and guidance from different people to help us with, ensure that we are compliant.

**Interviewer:** The last one is just in terms of the GDPR, how have the changes impacted the department?

**Interviewee 2:** Impacted the department? I think we’re going to have to have a much kind of more thorough process on, at the moment we very rarely get, like DSA requests, we very very rarely get them, so I think possibly now we’ll start getting more in because it’s more of a topic of conversation people may hear about more, so that’s something that well have to consider and make sure we have a process in.

**Interviewer:** Ok brilliant. The last section is just about the ramifications under the GDPR. So, the first one is, are you aware of the possible outcomes against the company if breach of legislation occurs?

**Interviewee 2:** Yeah, I know that there are some pretty hefty fines, I think they’ll be, probably a few years, I say a few years, they’ll allow people some leniency before the start kind of hitting people with those fines, but yeah, I think we really have to be strict with it to make sure people know where they stand from the start.
Interviewer: Ok brill. The next one is are you and other employees aware that you can be subject to liability personally for failure to comply and direct action can be taken by regulators, controllers and data subjects?

Interviewee 2: I didn’t realise that, directly.

Interviewer: Yeah, I think from the data protection act to the GDPR, whereas it used to be, just a data controller, the company can take action, it’s now the data subject and regulators, so the ICO, so I think that’s something that while I’ve been doing my research, that is one of the things that people may not be aware of.

Interviewee 2: Yeah. No, I didn’t.

Interviewer: Ok brill. And then the last one is how do you ensure you are fully compliant with the new legislation practice?

Interviewee 2: I think I need to re-read all the guidelines again. No, I think we need to have more conversations as a team to make sure, kind of that we are doing everything and the reasons we are doing it because I think sometimes people, you know, you do things just because you’re told, you need to make sure you chuck this away after 7 years, or you dispose of this, or you don’t send an email encrypted but I think, as a team we need to educate every one of the reasons behind it and what the ramifications are if you don’t do it, so yeah that’s something, I think both interviewee 1 and I have talked about, is kind of an education session.
Appendix L – Transcript from Interview 3

Interviewer: Alright, are you ready?

Interviewee 3: Indeed

Interviewer: Ok. The first is just for your approval to be recorded?

Interviewee 3: Yeah, that’s fine

Interviewer: And then the second one is that you’ve signed and acknowledged the consent form?

Interviewee 3: I have

Interviewer: Ok. So, the background questions. What is the organisation that you work for?

Interviewee 3: Information Commissioners Office, so the regulator of the DPA

Interviewer: Brilliant and what is your position within that company?

Interviewee 3: Lead Policy Officer and I’ve been here for almost 7 years, so not doing that role. I was initially the support officer for 5 and a half years and now I’m a Lead Policy Officer.

Interviewer: Ok brilliant. What does that entail?

Interviewee 3: So, a big part of my role is to go out and about and to help organisations get data protection right. So, we do a lot of awareness raising sessions, we don’t do training because we have to maintain that independence, but I primarily work with the voluntary sector, local government, so all to any local authorities will normally come to me as a point of contact. Private sector which is quite a big one in Wales because we’ve got so many kinds of SME’s that are, you know, interested more than ever in getting data protection right and the police and justice sector as well, but we kind of dip into, if I need to do something with education and health I will go and do an awareness session if one of my colleagues can’t. So yeah, quite a broad range but I am basically there to help organisations get it right and for them to contact if they need any kind of advice or guidance.

Interviewer: Ok brilliant. The next topic is about the GDPR, so why was the GDPR introduced?

Interviewee 3: I think one of the main reasons is to kind of bring the current data protection act up to, kind of, you know, the standard at the moment in terms of the technology that
we’re using. So, really to give it a 21st century approach to data protection, so if you kind of
think, so I should first of all start off by saying that the data protection act 1998 has been
around for 20 years this year and 20 years is quite a long time to have one piece of legislation
in place given the kind of amount that technology has grown since 1998, so an example would
be things like Facebook came in to existence a few years after the 98 act came in to existence,
so already a few years into the DPA 1998 you already had data being used and collected in
ways that probably weren’t foreseeable when the 1998 act was even drafted. So yeah, kind
of just to give it that 21st century approach to increase the rights that individuals have with
relation to their information as well.

**Interviewer:** Brilliant. So, the next one was what does it hope to achieve, but that’s probably
more what you’ve kind of covered with what you’ve just said.

**Interviewee 3:** Yeah, I think it’s there to kind of bring that consistency across the European
union and all the member states that are part of the EU. GDPR replaces what we call the 1995
data protection directive, so that directive required all EU member states to transpose the
directive requirements into their own domestic law so that UK have their DPA 1998. France,
Italy, Spain etc. would have had slightly different pieces of law. So GDPR for the first time
ever, will be, you know, it has direct effect across all EU member states, so it is going to be
really consistent approach to data protection, for the first time ever and not just in the EU,
obviously GDPR applies to those that are based outside of the EU that are processing the data
of EU member citizens. So, it hopes to achieve A that consistency, but its more than just the
European kind of approach, it’s that global consistency because GDPR will apply to so many
more organisations than just you know, domestic piece of legislation such as the DPA 1998
would have.

**Interviewer:** Ok brilliant. In regard to the DPA and the GDPR, what do you think were the
main changes from the two legislations?

**Interviewee 3:** Both pieces of law are based on principles, so on the current DPA you’ve got
8 principles of kind of good basic common-sense information handling practice. So you’ve got
things like make sure you’re processing data fairly and lawfully, don’t keep it for longer than
you need to etc. so luckily GDPR is still a principle based piece of legislation and when I’m
going out and about to organisations I always say that that’s a good thing because what it
does is it takes those principles and it puts them into the organisations court and says look, these are the principles of GDPR, these are what you need to comply with, but what’s appropriate for a small corner shop in Cardiff is going to be completely different in terms of the arrangements that they need to have at Cardiff and Vale health board for example and Cardiff Council. So, one piece of law, such of the GDPR, has to apply to all of those kinds of organisations. So, a kind of difference I suppose is yes they’re both principle based, GDPR takes it a bit further and really requires organisations to demonstrate that accountability, so it’s not just a matter of getting the principles right and you know, perhaps sailing along quite nicely because no one’s ever complained, you know you’ve never had to report a breach to us, it then takes it further and says yes you’ve got to comply with these principles but for the first time ever you’ve got that sudo-principle of accountability that says you’ve got to actively demonstrate how you’re trying to get it right, so you know, the importance there being got to have policies and procedures in place to help demonstrate to your data subjects, demonstrate to the ICO how you’re trying to get it right. Staff training is a big issue, we always expect all organisations to have trained every member of staff that deals with personal data on at least a yearly basis, so have that yearly training and refresh it where necessary. A lot of the areas are really similar but when I’m out and about a lot of people are panicking that some of the GDPR obligations are new, so things such as identifying your lawful basis under the GDPR, that’s not a new obligation whatsoever, because under the current data protection act you have always had to have lawful processing, so you’ve always had to have a schedule 2 condition for normal personal data and schedule 3 for more sensitive data, those two requirements are almost identical under GDPR because you’ve got to meet an article 6 basis and an article 9 basis for lawful process, um sorry for sensitive data processing sorry, so a lot of the similarities are still there. Things like breach reporting, we’ve always encouraged organisations to report breaches to us. GDPR takes it that bit further and says its mandatory, if a breach is likely to impact on the rights and freedoms of the data subject, whether that’s 1 or 10,000 individuals that have been affected, those need to be reported to us, for the first time ever, within 72 hours. Things like consent, there’s a much higher kind of standard of consent under GDPR, so at the moment if you’ve got an organisation that’s kind of using a pre-ticked box its not brilliant practice whatsoever in the current law but under GDPR that pre-ticked action would become unlawful, because consent under GDPR needs to meet a much higher standard in that it needs to be a positive affirmative action, so I as an individual have
got to either tick a box, verbally consent to something, basically just demonstrate that consent by me taking an action as opposed to kind of inferring consent by my silence or inactivity, so very much, you know a lot of similar principle based approaches between the two laws with a few tweaks here and there.

**Interviewer:** Ok brilliant. So, what do you think are the key challenges that companies will face in terms of updating their compliance?

**Interviewee 3:** I think that those companies that are currently, you know they’ve got a good grasp on data protection, they know the requirements of the current DPA 1998, those organisations will find the gap to jump on the 25th of May, that will be a lot easier to navigate. So, the key challenges I suppose are for those organisations that don’t have a good grasp on the current law, so things like not knowing what information they hold, because if you don’t know what data you’re processing, how can you be compliant in respect of having a lawful basis? Making sure that you’re helping individuals meet their, you know their strong rights under GDPR. So you know, the more organisations can get their house in order now, the stronger position they’ll be come 25th May this year, so yeah, if you’re getting it right now you’ll find that gap a lot easier to navigate.

**Interviewer:** Ok brilliant. That probably leads onto the next one, so what support and materials are out there to help companies comply with the new legislation?

**Interviewee 3:** So we’ve always had a really good helpline service in the ICO, so we always encourage organisations, if they’ve got any queries or concerns, give us a ring and whilst we can’t always say yes this is the right approach or no this isn’t, because again we’re the independent regulator, we are certainly here to help organisations and I think a lot of people are quite scared to perhaps contact the ICO but I would always encourage them to do so because we would much rather hear from you before something goes wrong, and we can hopefully prevent something from going wrong, than the first time you contact us, you know, it’s because something’s gone wrong because you didn’t pick up the phone. We’ve got a really good self-assessment tool kit that we really encourage organisations to have a go at, so that’s on our website, it doesn’t store any of the answers, its purely for that organisations own use to answer a few questions, print off the results and we’ll then kind of suggest bits of guidance that we think is necessary based on what that organisation has answered. We offer small kind
of audits called advisory visits, they’re tailored towards more the kind of smaller
organisations, so we do audits with bigger public sector organisations, big private sector firms,
but advisory visits are certainly a tool that we often use to help out those smaller
organisations to assess their current compliance and to kind of, suggest gaps where we think
they might be, not getting as brilliantly as they could be now, but we’ll suggest in our advisory
visit report, areas where we think they can improve. Our website has got a range of guidance,
so we’ve got the guide to GDPR, which basically, that guide is kind of, most of my
presentations when I go out and about and talk about GDPR over the last 18 months, two
years, has been taken from the guide to GDPR, so I can’t stress how important that is for
organisations. And then we’ve got tailored advise for each sector, so if you go on our website,
you know if you’re a local authority you can click through to local government pages, charities,
I think micro-businesses was launched a few weeks ago, so you know for those really small
organisations which there are a number of in Wales, GDPR might seem a bit daunting, so you
know going on that page, it really explains quite easily the key areas to try and prepare in
terms of getting it right under GDPR, and the 12 steps to take now, guidance that we’ve had
around, I think we’ve had for around 2 years now, that’s a really key document because it sets
out 12 steps that organisations absolutely need to look at before 25th of May, because if they
look at it on the 25th then you know, it’s too late then because you need to use this time to
prepare.

Interviewer: Brilliant. So the next bit is about failure to comply. So the first one is what are
the ramifications if a company does comply with the GDPR?

Interviewee 3: They’re very similar to what we see now. So, we use a kind of range of
resources available to us. I should kind of say first off that we always, we prefer engagement
over enforcement, we much rather use other tools available to us than go down that route of
kind of, you know, enforcement, our formal powers of enforcement. Yeah, the powers are
very similar to the current data protection act, so we can issue what we call information
notices, so if we need information from an organisation and there’s that kind of reluctance to
give us certain information, we can issue them with information notice which compels them
to disclose data to us. That’s quite rarely used because most organisations will you know,
voluntarily give us that information to try and get things right, because they also are in a
position where they want to get data protection right as well. We can issue undertakings, so
it’s kind of agreement between us and an organisation to try and commit to getting things right. So, we might say, you know, within 6 months we want you to have trained all of your staff, if we need to be a bit firmer and you know, the breach that we’re looking into was quite serious, we might issue an enforcement notice. So that notice will legally oblige an organisation to take certain steps, so it could be, you will train all of your staff within 3 months, or you will stop processing data in this way because it might be unlawful for example. And in the most serious kind of examples, so when the data controller, so the organisation ought to have known that there was a high likelihood that something was going to go wrong and it has gone wrong, then we can issue civil monetary penalties, so at the moment we can issue fines of up to £500,000. Under GDPR, they go up, well they kind of increase quite significantly, to up to 20 million Euro in the top tier of breaches, to 4% of annual global worldwide turnover. So yeah, whilst most the powers are similar, it’s that kind of increased amount that we can fine that a lot of people are focusing on under GDPR.

**Interviewer:** Ok. So, going on from what you kind of just said, why were the ramifications altered from the Data Protection Act?

**Interviewee 3:** I think the increased fines that we see under GDPR really do reflect the importance of personal data, so to me, when I’m giving my information to an organisation, I treat my data as an asset because I wouldn’t want to give my data to company A that’s got no kind of accountability, no staff training in terms of data protection, they’re not following the principles of any kind of data protection legislation. I’d much rather give my information to organisation B that’s going to treat my data as an asset, you know, as the asset that I think it is. So, I think the increased fines really do reflect the importance of getting data protection right because you know, a 20 million fine looks a lot more scary and more of a deterrent than perhaps a half a million fine might be to those bigger organisations where half a million pounds won’t be as much of a deterrent as perhaps it should be. I should say as well that although people are focusing on those increased fines under GDPR, we’ve had a series of myth busting blogs on the ICO’s website, so our commissioner Elizabeth Denham has written a few blogs, one of them was focusing on the fact that people do think GDPR is all about fines and you know, that we’re going to go out there after GDPR comes in and make examples of organisations. That’s absolutely not the case, so its again, I said that we prefer engagement over enforcement, we don’t like to be in a position where we have to fine but if we are left
with no other choice, that’s the route that we have to go down. So CMP powers are there to be used when necessary but we do have a range of kind of other options available to us and you know, GDPR isn’t about putting organisations out of business, it’s about making sure that they’re treating personal data as the important asset that it really is.

**Interviewer:** Ok brilliant. So, the last one is just in terms of the future of the GDPR. So, do you think all companies will be fully compliant by 25th May?

**Interviewee 3:** It’s definitely within their interest to be fully compliant because 25th May onwards, if anything happens to personal data on 25th May, 26th May, anywhere down the line after that date, the GDPR is the law that we’re going to be regulating. So, the DPA will be repealed, we will be looking at complaints that happened 25th May onwards under GDPR. So, it really is in everyone’s interest to be compliant by that date, which is why the importance of following those 12-step guidance, looking on our website, doing a gap analysis in terms of where you are now with the data that you hold and where you need to be by the 25th. So, I would urge all organisations that haven’t thought about GDPR, as a kind of necessity to start looking at the requirements now and make sure their houses are in order on 25th.

**Interviewer:** Ok brilliant. The next one is what will happen to the GDPR when the UK exit the EU?

**Interviewee 3:** So, because the regulation is an EU regulation, it has direct effect in all member states without member states having to kind of transpose the law into, you know, their own domestic laws. Obviously, so 25th May we’ll still be EU members so that law will have direct effect. When we do leave, the GDPR will become enshrined in UK law, not through the data protection bill that’s going through parliament now, but by the European Union withdrawal bill, which when it becomes an act, that will be the law that will then enshrine the GDPR into UK law basically. So, again it’s in everyone’s interest to get GDPR right because it will be around, it’s not a matter of you know, we’re going to be leaving the EU so we don’t need to worry about GDPR. It is absolutely essential that by 25th May, organisations are aware that that will be the law that the UK supervisor authorities, so the ICO, is regulating.

**Interviewer:** Ok brilliant. And then the last one is, what is the future for data protection within the UK?
Interviewee 3: So, you’ve got the data protection bill going through parliament that I mentioned in the last question. When that receives royal ascent, it will become the Data Protection Act 2018. So, it’s that law that’s going to equip the UK with robust data protection laws, so it will future proof us in terms of data protection. The bill itself addresses areas which are left to the discretion of the, each member state, so for example, GDPR says that if you’re using an online service and you’re targeting that at children, then actually, if the child is under 16, so 16 or under, each member state can kind of determine at what age they think that that child needs to have parental consent, so the data protection bill addresses areas such as that.

So in the UK, it will be if the child is under 13, then that’s when parents will need to consent on children’s behalf, in relation to online services such as information society services. It addresses areas which are outside of the scope of GDPR, so for example personal data processed by intelligence services and it also transposes the law enforcement directive into UK law. So, because the directive requires that domestic legislation to kind of implement it into member state law, that’s what the data protection bill, or the Data Protection Act, when its passed by parliament, that’s what that will do, so I think the future for data protection in the UK is very strong. We’re having that update that we’ve been kind of wanting for a few years because of the change in technology, so I think the future looks really good in terms of data protection within the UK.
Appendix M – Transcript from Interview 4

Interviewer: Are you ready?

Interviewee 4: Yep

Interviewer: The start is that you’ve approved the recording of the interview?

Interviewee 4: Yep

Interviewer: and that you’ve signed and acknowledged the consent form?

Interviewee 4: Yep

Interviewer: The first questions are just background questions, so what is your position within the company?

Interviewee 4: I am a HR advisor

Interviewer: and how long have you been doing that for?

Interviewee 4: I have been with the company for just over 8 months

Interviewer: and what does that entail?

Interviewee 4: It is day to day activities, anything relating to employee relations, so disciplinaries, grievance, attendance

Interviewer: Ok, brilliant. This section is regarding the current data protection procedures, so what employee data do you hold?

Interviewee 4: We hold a lot of employee data, and that is broken down into personal and sensitive data. So personal data would include name, address. The sensitive data would then include things like gender, ethnic origin and salaries.

Interviewer: Ok brilliant, how do you ensure the safety and security of that data?

Interviewee 4: There are nine people within the HR Team, and we are the only ones that have access to sensitive data. So, line managers or operations wouldn’t be able to look at things like salaries, it would only be us. So, anything to do with payroll is through the HR team. We run payroll ourselves so it’s more of a tighter control. We do get requests from managers for absences within their team but we would only give that out by validating who is asking for it.
Interviewer: Ok, what data protection policies do you currently have in place?

Interviewee 4: We’ve got a data protection policy, we’ve got a data retention policy, the majority of things though are covered under the employee handbook. And we also do a data protection e-module.

Interviewer: Ok, brilliant. Kind of what you’ve just mentioned, the next question was about training and if so when is it reviewed?

Interviewee 4: We’ve got an E learning module which reviewed every 2 years.

Interviewer: Ok, brilliant. In terms of current data protection procedures, what is the biggest challenge right now?

Interviewee 4: right now, we still have an awful lot of paper files for older employees, so obviously business has grown massively in 2016. So, the older employees we have paper copies for. So that is our biggest challenge at the moment.

Interviewer: Ok, the section is about the GDPR. When did you first hear about the change in the legislation?

Interviewee 4: probably about July 2017, I was off work for about six months so it would have been around the time I went back to work.

Interviewer: Ok, brilliant. What did you identify as the key changes of the legislation?

Interviewee 4: probably about 80% of what we already do is covered by the existing DPA (Data Protection Act) but we do have to relook at things such as consent forms we use for vetting, they need to be much more explicit. We’ve had to review our employment contracts, our onboarding forms, making people well aware of what we will be requesting and that we do a follow up 2-year vetting. We need to make sure we’ve got the correct DSAR process in place, because obviously that is changing, there’s will be no fee. And also, because we’ve got L&D within the HR function we need to make sure all of our modules are updated in line with the new process.

Interviewer: Ok, brilliant. How have the department dealt with these changes?

Interviewee 4: So, the company has a GDPR project team. Whereby there will be representatives from each of the departments. Our HR business partner is on that project
team, so we rely heavily on him to come back and update us. And that is normally through
the course of things like emails, team meetings that we have every week so he will feed in
any changes. Also, our HR director is on that project team, so she has a big impact on what’s
going on.

**Interviewer:** Ok, did you use any techniques or tools or materials to help support the change?

**Interviewee 4:** Working within the HR function, we have access to quite a few external
websites so we have regular updates from Xpert HR, we also have Huw James solicitors, ACAS
and the ICO produced a 12-step information sheet on what organisations need to do. So,there is plenty of external support.

**Interviewer:** How have these changes impacted the department?

**Interviewee 4:** as mentioned earlier, we’ve got quite a considerable amount of paper files
remaining, so we’ve actually employed a temp, and what they are doing in scanning all
existing paper information that we have and that information is then saved in a shared drive,
which only nine people within HR have access to.

**Interviewer:** Ok, brilliant. The last section is just about the ramifications if failure to comply.

So, are you aware of the possible outcomes against the company if a breach of legislation
occurs?

**Interviewee 4:** yes, currently there are fines but with obviously following the introduction of
the GDPR these fines will increase considerably.

**Interviewer:** Ok, are you and other employees aware that you can be subject to liability
personally for failure to comply and direct action can be taken by data regulators, controllers
and subjects?

**Interviewee 4:** initially no, but I think that there has been so much information that we have
read up on in regard to the changes that it then came to light through them changes.

**Interviewer:** the last question is that how do you ensure that you are fully compliant with the
legislation in practice?

**Interviewee 4:** we get regular updates from the HR business partner after the meetings, as I
said we’ve also got a lot of external information available to us, we do rely on the GDPR
project team to send out regular comms to the site, which they do. And that were on top of everything in regard to our policies and that making sure their reviewed and update.