Sheffield Hallam University

Impact of EU-GDPR on local authorities in England : an investigation into how the introduction of new EU data protection legislation will affect Local Authorities in the UK and what the key changes will be that this new law will force on these organisations.

ADSHEAD, Deborah.

Available from the Sheffield Hallam University Research Archive (SHURA) at:

http://shura.shu.ac.uk/20711/

A Sheffield Hallam University thesis

This thesis is protected by copyright which belongs to the author.

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author.

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given.

Please visit http://shura.shu.ac.uk/20711/ and http://shura.shu.ac.uk/information.html for further details about copyright and re-use permissions.

COLLEGIATE CRESCENT
SHEFFIELD S10 2BP

102 114 755 9

ProQuest Number: 10702809

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10702809

Published by ProQuest LLC (2017). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

Impact of EU-GDPR on Local Authorities in UK

An investigation into how the introduction of new EU data protection legislation will affect Local Authorities in UK and what the key changes will be that this new law will force on these organisations

LLM by Research Thesis

By

Deborah Adshead PC.dp, FHEA, PgCert, BSc

Supervisor: Alan Reid

12 August 2016

Impact of EU-GDPR on Local Authorities in UK
LLM by Research Thesis

By: Deborah Adshead
Supervisor: Alan Reid
Date: 12 August 2016

Foreword

During the time of writing this thesis the circumstances that led to this research being undertaken in the first instance have changed dramatically due to the results of a referendum held in the UK on 23rd June 2016 to determine the fate of the UK in the EU.

Since the majority of the population voted for the UK to withdraw from EU membership the economic, political and legal circumstances have changed quite dramatically.

At the outset this research project was to look at the implementation of the new EU data protection legislation in the UK and to undertake a gap analysis between the existing and forthcoming laws to determine just how much of an impact the new law was likely to have on the local authorities. However, given the changed environment it has been necessary to adjust the scope of this project somewhat.

The referendum took place several weeks prior to the submission date of this research project therefore much of the information on the current situation is fluid as the immediate future for data protection legislation is still uncertain. Under the circumstances it seemed more appropriate to spend the time remaining before the submission deadline to revise some of the findings of the research and focus some effort into researching the possible outcomes of this decision and some of the issues that may arise from the new situation the UK now finds itself facing.

Therefore, it is pertinent to state early on that, whilst the information on the legislation and the timeline of the implementation of the EU – General Data Protection Regulation (GDPR) still remains correct, the findings and recommendations section relating to the implementation of the GDPR on local authorities would only now be relevant if the UK were to adopt the GDPR in its entirety and enter into some agreement with the EU to enter into a One-Stop-Shop regulatory solution and that all parties agree to extend the EU-US Privacy Shield agreement to include the UK.

Having said that, all efforts will be made to ensure this research project is as current and relevant as possible and to identify possible issues that may arise from the referendum results and any potential course of action that could subsequently be taken, despite the time constraints imposed on completing it.

Impact of EU-GDPR on Local Authorities in UK
LLM by Research Dissertation

By: Deborah Adshead
Supervisor: Alan Reid
Date: 12 August 2016

Abstract

This research explores the EU General Data Protection Regulation (2016/679) (GDPR), due to come into force in May 2018, and its impact on UK local authorities.

Its key objectives were to identify how the pending changes to data protection legislation might impact on current compliance procedures and policies. Its aim was to provide recommendations for local authorities regarding the key issues in order to minimise the risk of non-compliance with the new law by being better informed of the obligations the new rules impose on data controllers.

The study first looked at the structure of the EU and the procedure for introducing new laws, to understand the provenance and supremacy of the legislation. It then looked at the political and legal background regarding data protection and compared the previous and existing legislation to the new Regulation to evaluate the amount of change likely.

Consideration was then given to the current compliance situation in local authorities. Studies conducted by the ICO and Big Brother Watch identified major problems in some local authorities with breaches of the Data Protection Act resulting in considerable fines totalling in the millions.

Whilst key principles of data protection will remain the same the new regulation will introduce important changes requiring greater vigilance over compliance if fines are to be avoided. One is the compulsory requirement to report data breaches, which could pose a serious problem in many local authorities. According to Big Brother Watch, 38% reported never having had a breach; at best this means they have little experience of dealing with one, at worst there could be more fines to come.

The new law imposes a distinct change of direction, from educating organisations after a breach has occurred to requiring proof they took adequate measures to avoid one. This will necessitate implementing clear policies, recording any incidents, training staff adequately and having full accountability throughout the organisation. To avoid further losses to public sector services it is essential that local authorities make the needed changes to meet the new law.

Table of Contents

1. Introduction

Data is the gold of the 21st century; its mining is the collection and profiling of that data and the gold rush is the sharing and application of the actionable information the mining activities produce. Once data's worth was recognised those companies at the forefront of the realisation of the potential for data to be monetised, such as Google and Facebook, started to collect what they could get their hands on, mine for what they couldn't and hoard data to increase the overall market value of their companies. Some of those companies now have stock market values comparative to the worth of a small nation. Throughout these pioneering years of the information revolution however little consideration has been afforded to the cost to the civil liberties of the data subjects whose information is slowly being pieced together as technological advances allow companies to build richer pictures of people's lives. As targeted marketing using data-mining profiling techniques became more commonplace, and it was evident that data was being shared by organisations often without the consent of the individual, the public started to get uncomfortable by just how much private information organisations had access to.

Whilst it may be too late to return to times when shutting the bedroom curtains was all one needed to do to ensure absolute privacy, there is recognition by governments and citizens' interest groups worldwide that allowing the current practices to continue unchecked and unregulated could cause serious damage to the fabric of society. Data protection legislation is governments' answer to this problem. As flawed as some may see it, it does allow some redress to the individual who without it would have to resort to civil action against each company deemed to be invading his/her privacy.

1.1. Overview

After four years of negotiations and much lobbying, in April 2016 new data protection legislation was finally adopted by European government. The reform concerns three pieces of legislation, a Regulation aimed at both the private and public sectors, a Directive to facilitate greater cooperation in police and criminal justice matters, and a Directive to strengthen national security in member states by sharing of Passenger Name Records. The Data Protection Regulation 2016/679 (the "Regulation"), was purportedly due to be implemented by the end of 2015, but Deputy Commissioner and Director of

Data Protection, David Smith (2015) was much more pessimistic and expected to see a final document by 2017. After an implementation grace period of two years, the new Regulation will finally enter into force replacing existing data protection laws in all EU member states on 25 May 2018. For various reasons explained in due course the impact of the Regulation alone will be the main focus of this thesis.

The current EU Data Protection Directive (95/46/EC) (the "Directive") provides a set of minimum requirements that all EU countries must meet. However as a Directive rather than a Regulation, it leaves it open to member states to develop their own laws within the framework provided. Consequently, levels of protection afforded data vary across the EU and interpretation and enforcement issues exist that have ultimately led to differing compliance requirements across member states. In the UK the Government repealed the Data Protection Act 1984 and ratified the EU Directive by introducing the Data Protection Act 1998 (the "Act"), thereby cementing the EU obligation in UK law. However, the Act has invited criticisms from the European Commission (EC) regarding its effectiveness, who issued a number of 'reasoned opinions' since 1998 citing a failure to comply with the Directive's requirements (European Commission 2010). Often seen as a precursor to legal action being undertaken in EU Courts the official memos prompted the UK Government to make some amendments to the Act, but still not enough to satisfy the EC.

The EC has expressed particular concern over the power of the UK's enforcement body, the Information Commissioner's Office (ICO) to impose effective compliance measures and penalties on organisations. Current practice of voluntary breach notifications falls short of criminalising individuals for breaches of the Act; information and enforcement notices and monetary fines imposed by the ICO are the main punishment when breaches the ICO is informed of do occur. In the private sector where fines affect profit a fine may be enough of an incentive to implement robust compliance measures (particularly since the maximum fine has recently been significantly increased); the potential damage to a company's reputation another. However, in the public sector these possible consequences do not have the same impact, particularly given that any financial penalty imposed is ultimately paid by the taxpayer, the victim of the wrongdoing! In a report on the findings of a survey of 16 local authorities, the ICO (2014) stated that in 2013 almost £2.3M had been levied from the public sector alone, which inevitably impacts frontline services.

Lloyd (2014 pp59-60) argues that the general absence of criminal sanctions in the current legislation is somewhat justified given that "...the Directive and the Act are to a considerable extent surviving dinosaurs from the age when computers were mainly free-standing [business] machines...with limited networking capabilities" and most websites the product of hobbyists. The data landscape has changed significantly since their inception. The widespread adoption of information technology, exponential growth in the use of the Internet and cloud storage providers have all contributed to a culture of data capture, processing, storage and sharing that has little regard for sovereign borders and poses many security risks.

The new Regulation is intended to strengthen the protection afforded to individuals in this new technological paradigm whilst simultaneously making it easier for organisations to realise the potential that new data management technologies offer. How well the Regulation meets this goal remains to be seen but there are a number of areas that the Regulation does not appear to provide adequate clarification on, which is a cause for concern. With an increase from 34 articles in the Directive to 99 in the Regulation, Koops (2014) is certain that legislation he states is already too complex for many outside the legal profession to grasp is about to become even more so, thereby increasing the risk of widespread non-compliance. Article 31 of the Regulation introduces the statutory requirement of notification of data breaches but Treacy (in Carey 2015 pp131) warns it has the potential to overwhelm the ICO with notifications as the proposal "does not specify the criteria for deciding what constitutes a data breach, and so there is no 'de minimis' provision."

In the private sector competitors offer alternatives to poor data management, however, other than opting out altogether, there is no alternative to interacting with local authority systems; especially if there is a legal obligation to do so, such as registering a birth. It is therefore even more important that compliance policies and procedures implemented are robust and that safeguards are preventative and actually minimise the risk of breaches occurring.

1.2. Aims and Objectives

So far, there is very little in the way of guidance on the imminent changes for local authorities who are in a great state of technological flux as, in an attempt to make cost savings, services are going digital wherever possible supported by legislation under consideration in Parliament, the Digital Economy Bill. With over 4 million employees working in over 400 local authorities across the UK, many of which contract out IT services to third parties, this inevitable data security risk furthers the need for adequate privacy safeguards to be firmly embedded everywhere in the public sector. It is essential that those able to access the data take every precautionary measure to ensure it remains uncompromised. Article 30 of the Regulation extends the obligation to demonstrate adequate security measures to both the Data Controller (the entity legally responsible for defining what data is processed and how) and the Data Processor (any entity excepting employee(s) of the Controller undertaking data processing functions on behalf of the Controller). According to Treacy (in Carey 2015 pp129) this "is likely to lead to a reassessment of risk, and the reallocation of risk in outsourcing and other contracts."

This research aims to identify and assess those risks involved in implementing the new Regulation in local authorities and the potential impact on data management and maintenance therein. It aims to:

1. identify key changes in the new legislation by undertaking a detailed literature review of the legislation;
2. investigate legal cases in the UK and EU related to the key changes;
3. make recommendations as required regarding potential areas for concern by producing a summary of changes required in compliance procedures and policies.

1.3. Terms of Reference

This is an academic research project completed for submission as the assessment instrument for the Master of Laws by Research (LLMRes) degree course. As such it is aimed at providing proof of understanding of the legislative landscape and procedures that have led to the decisions made to implement the new data protection legislation. The LLMRes is a part-time course with no taught modules and, as such, all the learning

undertaken to understand legal concepts and structures has been done on an individual basis through extensive reading of legal materials and use of reference books.

It was written for the academic assessment panel, in context of the above but would also prove useful reading for anyone requiring an introduction to data protection laws in the UK and EU. It may prove a useful starting point for a local authority wishing to further its understanding of the new EU data protection legislation but concepts and recommendations are rather broad and general and, as such, should not be relied upon as providing an accurate summation of a situation for any one organisation as this may differ from Data Controller to Data Controller. It is not intended to be utilised as legal guidance. Anyone wishing to act on any recommendation in this thesis is advised to seek additional and independent advice on their individual circumstances.

1.4. Scope

The research covers the background of data protection legislation and the global, European and UK policies that have resulted in the data protection landscape presented today. It also depicts the key events leading to the creation of the EU structure in existence today and how legislation is created. This is included to provide recognition of the supremacy of EU law and when and how the UK is able to deviate from adopting legislation originating from the EU.

It then looks at the development of key pieces of legislation specifically related to the protection of data before discussing the requirements of the Data Protection Act 1998 (DPA), the current legislative instrument in the UK, introduced to enact the data protection Directive 95/46/EC and some of the rulings of the ECJ that have led to considerable changes. The new data protection reform legislation is then discussed and compared with the Directive and the DPA.

Before discussing the compliance requirements of Local Authorities and drawing some conclusions on the success or otherwise of these organisations to avoid breaches, it was important to add a section on the changed landscape resulting from the decision in the UK Referendum to withdraw from the EU and how this might affect the data protection framework in the UK. Some options for various paths that could be taken are briefly considered.

The thesis concludes by summarising the key findings of the new Regulation in relation to the impact this is likely to have on Local Authorities in the UK should it, or similar legislation, be adopted.

Whilst some secondary legislation is discussed it is outside the scope of this thesis to cover any of this in any detail. Another key piece of legislation that will only be touched upon in passing is the Police and Criminal Justice Directive 2016/680, the second key piece of legislation that will come into force alongside the new Regulation, and Passenger Name Records Directive 2016/681 (PNR Directive).

This dissertation does not constitute a detailed discussion on all of the judicial rulings related to data protection; only those that have had a significant impact since the Directive was enacted and have led to the development of the Regulation have been covered.

2. Research Methodology

This section of the report will discuss some of the approaches and methods used to uncover the information required to undertake this research in order to make the relevant compliance recommendations to Local Authorities.

2.1. Research Approaches

There are a number of ways to approach a research project depending on the nature of the information under enquiry and the outcomes required. Legal research is a specific discipline that necessitates particular approaches to finding and compiling information. The key approaches are described below.

2.1.1. Doctrinal Research

Doctrinal research is also known as the "black letter" approach to legal research and is perhaps the most common approach known to legal scholars. It focuses on the state of the law as it currently is and how it has developed. According to McConville and Chui (2007 pp19) the objective of using this type of research method is to define a particular area of law and its application by analysing the legislative instruments, case law and judicial arguments relating to the topic. They state that this "is often done from a historical perspective and may also include secondary sources such as journal articles or other written commentaries [...and researchers may...] also provide an analysis of the law to demonstrate how it has developed in terms of judicial reasoning and legislative enactment."

This research was undertaken using doctrinal methods. Legislation and case law was analysed to present the current data protection law in the UK. For the purposes of this research this approach was used to discuss the development of data protection legislation from its early forms to the latest piece of legislation to come out of the EU and to compare the two.

EU legislative authorities were identified within the research including their publications and explanations regarding the new data protection laws. These were reviewed and compared to the current UK Data Protection Act 1998 to determine the differences between these two pieces of legislation and highlight the key changes likely to be required in the UK once the new EU rules come into force. In order to determine where

primacy lies in EU law and under what circumstances it was necessary to provide a breakdown of the development of the EU judicial system, the types of legislative instruments at the disposal of the EU, and the relevant case law.

2.1.2. Non-Doctrinal Research

According to McConville and Chui legal research can be categorised as doctrinal and non-doctrinal. They define non-doctrinal research as a generic grouping of other types of research that is required to contextualise purely "black letter" research. Some types of non-doctrinal research, such as Problem, Policy and Law Reform research are not mutually exclusive and it is not unusual for these three non-doctrinal approaches to be used alongside doctrinal research where circumstances require a broad understanding of law in action. They explain that a project could commence "by determining the existing law in a particular area (doctrinal) [...then...] by a consideration of the problems currently affecting the law and the policy underpinning the existing law, highlighting, for example, the flaws in such policy. This in turn may lead the researcher to propose changes to the law (law reform)." (2007 pp20)

At the time of undertaking this research the forthcoming EU Data Protection Regulation was in flux and now, given the UK referendum results pointing to the UK leaving the EU, it is unclear whether the new legislation will be applied in the UK. It was therefore necessary to discuss policy in the area of data protection to make some determinations regarding the approach that should be taken by the UK authorities. In order to do so, it was important to discuss the area of data protection in relation to the application or non-application of the Regulation and the legal problem that either approach would represent.

2.2. Qualitative and Quantitative Methods

The key differences between qualitative and quantitative methods of research relate to the analysis of discussion compared to the analysis of numerical data. Each method would produce very different results. With qualitative methods the outcome is a narrative analysis of the written or verbal text, whereas the outcome of quantitative methods is an analysis of the numerical data observed.

An example of qualitative research methods include: written documentation; interviews; and open-ended questions within a survey. With each of these methods there is a

dialogue, either written or aural, that can be analysed for the use of language and semantic meaning and interpreting meaning from this analysis. In this regard, it can be argued that doctrinal legal research can be seen as qualitative methods of research. McConville and Chui see this to be the case as simply presenting information found in the process of undertaking legal research is not enough in itself. They put forward the following argument that this is due to the, "process of selecting and weighing materials taking into account hierarchy and authority as well as understanding social context and interpretation." (2007 pp22).

Quantitative research, by contrast, is more concerned with the predictability or otherwise of a given situation when analysed in context of specific criteria and compared to other situations where similar criteria may be present. Examples of this type of research method would include: the results of a survey with closed questions; the number of times an outcome to a given set of actions is observed; or any other occurrences that can be counted. In the context of legal research, this type of research method may be used to measure and compare sentencing for similar crimes across regional courts or by different judges.

2.2.1. Qualitative Research

As well as the doctrinal research, compliance requirements within local authorities was researched by reviewing guidelines issued by the Information Commissioner's Office (ICO), the body tasked with the authority to oversee data protection compliance in the UK. Further consideration was given to any mandates from Government to local authorities necessitating they provide a greater level of compliance than required by law.

2.2.2. Quantitative Research

Finally, penalties issued by the ICO and cases that have been brought before UK and EU law courts dealing with data breaches, in particular those that have occurred within local authorities, were reviewed to determine the factors in data breaches that lead to the most severe penalties. These findings were used together with the review of the key changes in legislation to form the basis of the recommendations to help ensure local authorities pay greater attention to those areas of compliance that meet the needs of the new legislation and that are able to either cause the most financial or reputational damage to the organisation or where policies and procedures are currently non-existent.

3. Background to Data Protection in UK

The earliest data protection laws came into force in 1984 in an attempt to offer some basic protection and recourse in law if a company holding information on an individual failed to use it appropriately. However, over two decades of discussions, proposals and agreements preceded the 1984 legislation being implemented. Since that first piece of legislation there have been many changes resulting in new laws being passed and the domain of data protection has changed significantly over time, due to a variety of factors, some of which will be explored in this section.

3.1. Global Agreements

In 1948 the General Assembly of the United Nations adopted the Universal Declaration of Human Rights, formulated as a direct result of the atrocities committed in World War 2, in an attempt to bring about a more peaceful and civilised co-existence between nation states and offer citizens of the signatories of the declaration some safeguards about how they could expect to be treated by rulers of those nations. There are 30 articles in the DHR, which was adopted by 48 of the General Assembly members, with 8 abstentions including USSR, South Africa, Saudi Arabia and Yemen. Article 12 in particular is of historic importance to the DPA. It states that no individuals "shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks." It is with this backdrop that the UK and other countries independently started to develop legislation specifically designed to provide this protection. This is discussed further in Section 3.3.

Moving forward seven decades there are clear signs that organisations such as the UN, founded on the principles of global cooperation, have helped to foster an understanding of the necessity to have some standards for all nations around the world to adhere to. However, despite the objective of member states to meet a UN Resolution, in practice it is not that easy to force a country to abide by a UN ruling if they choose to ignore it. Legal rulings on whether a UN decision has been breached falls to the International Court of Justice (also known as the World Court) and the types of punishments it can dispense are somewhat limited and success in administration of sentences depends very much on the standing of the member state(s) in question in the world order. It is clearly

not as simple as imposing the types of penalties given to an individual who breaks the law, and attempts to compel countries to conform to a decision taken by other member states have had varying degrees of success. Punishments are much more effective if the state(s) under scrutiny can be persuaded or coerced into amending its course of action rather than being forced into it, especially in the case of one of the world's "super powers". Despite there being majority agreement on the use of torture, for example, some countries still show evidence of employing torture tactics despite being a signatory of the Resolution (UN A/RES/39/46) and there is little appetite for taking some of these governments alleged to be guilty of these acts (such as the USA, Russia and China) to task. Penalties incurred for not conforming to a UN ruling can include trade sanctions, having UN observers present in the country/area under investigation and, as a last resort, military intervention by a coalition of member states' forces. It can be said therefore that the UN is a valuable forum for cross-border discussion that can impose some changes on some countries but it does have its limitations when it comes to larger states with considerable military power.

A more effective approach to collaboration, although not the only one, has been the expansion of global trade. Many companies now operate on a multinational level as a result of the negotiation of trade treaties and relaxation of laws; this has allowed some companies to have a significant amount of lobbying power and influence over government policies in the countries they trade in. Many others, large and small, serve customers across the globe, aided by the invention of the Internet and the rise of the role of technology for trade.

The very infrastructure of the Internet lends towards cooperation as data passes (mostly) unfettered across sovereign borders. In order to benefit from the advantages a global network can offer organisations and citizens alike some agreement needs to be arrived at on how the components that constitute the network are regulated and kept secure; this includes the data that traverses the Internet.

A continuing discussion regarding the expansion of the Internet is the need to safeguard the privacy of individuals enshrined in Human Rights legislation. As a result of this need to ensure the end-to-end integrity of data, the Organisation for Economic Co-operation and Development (OECD) – a voluntary membership organisation comprising 35 countries who, in their own words, "help governments foster prosperity and fight poverty

through economic growth and financial stability [...and...] help ensure the environmental implications of economic and social development are taken into account." – helped to create the Global Privacy Enforcement Network (GPEN) a special interest group to share best practice, develop priorities and support joint enforcement initiatives. GPEN is an informal network of data protection authorities from countries across the globe (not limited to members of OECD) who when the need arises will meet to coordinate actions to limit the abuses of data privacy from governments, companies and technologies.

An example of this global cooperation is the "Privacy Sweep" research undertaken annually by all the member authorities. In 2016 the subject was children's online privacy particularly how websites and mobile phone apps target children and how children's details are then shared with third parties. The alarming results have helped participating authorities to consider reforms to current legislation to ensure specific rights for children, as discussed further in Section 6.1.3.1. The next "Privacy Sweep" will be looking at the Internet of Things, which will pose its own set of unique data protection issues that will need to have some collective governance agreed upon.

The OECD was also instrumental in developing some of the earliest data protection legislation in 1980 when it produced their Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The OECD guidelines were aimed at strengthening the protections of individuals' data from "the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data." Its aim according to the preamble on its website (OECD, 2013) was to "help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data ... represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries..." that were yet to implement such legislation. Aside from them not being binding in law, the key difference between these guidelines and the legislation that was introduced throughout the EU and other countries worldwide is the approach towards the perceived need to protect the data. Rather than stating that the protection should be a fundamental right, as in the EU legislation, it takes a more risk based approach to protection deeming it necessary dependent on "the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."

3.2. European Actions

The legislative relationship between the EU and its member states is a complex one that has evolved over time as increasing powers to make and enforce laws have been devolved to Brussels. This section will outline the structure of authority within the EU, its legislative relationship with the UK and describe the law-making process within this structure.

Given the recent decision of the UK to leave the EU (see Section 7 for more on this subject) it is still unclear exactly what the relationship between the UK and the EU will look like moving forward. However, for the foreseeable future the structure described in the following section is the status quo and laws introduced through the EU remain supreme.

3.2.1. Difference between Europe, the EU, the EEA and the EFTA

Opinion varies on the actual number but according to the United Nations, geographically Europe consists of 43 countries. Of those 43 countries several remain fully independent of any agreements with other European countries to: share policy decisions; produce common laws; and/or trade goods without the imposition of import/export tariffs. The three common agreements forged between the European countries are the European Union (EU), the European Economic Area (EEA) and the European Free Trade Area (EFTA). Each of these will be described in this section; it may well be that the negotiations to leave the EU see the UK adopting a similar approach to a country in the EEA or the EFTA, which would have an impact on legislative matters.

European Union

The European Union (EU) is a political and economic coalition of 28 member states that are located primarily in Europe. It comprises of seven institutions that together and with the cooperation of the national parliaments of all 28 member states produce common policies and legislation designed to facilitate trade, free movement of goods, people and capital, and to promote democracy and human rights both within its own member states and in other countries it deals with collectively. The single common market allows member states to buy and sell goods to a marketplace of over 500 million people without the imposition of import/export tariffs, the cost for that is the ceding of some of the powers of the national parliaments to the EU Institutions.

These Institutions are:

- the European Council;
- the Council of the European Union;
- the European Parliament;
- the European Commission;
- the Court of Justice of the European Union;
- the European Central Bank; and
- the European Court of Auditors.

Each of these Institutions and how they work together to create legislation and policies is discussed in more detail in Section 3.2.3. Section 3.2.2 is a summary of the key events that led to the creation of the EU.

European Free Trade Area

The European Free Trade Association (EFTA) today consists of four European states: Iceland, Liechtenstein, Norway, and Switzerland. It was created as an alternative to the creation of the European Economic Community (See Section 3.2.2 for more details on this). EFTA jointly negotiate free trade agreements with countries but don't have a customs union so some import/export tariffs are applied in certain areas of trade. Switzerland has a number of bilateral agreements with the EU that allow it access to the EU's marketplace but the remaining 3 countries have selected to be members of the European Economic Area (EEA) to gain access.

European Economic Area

The European Economic Area (EEA) was created by the EU in 1995 to provide a single market comprised of all EU member states and those members of the EFTA that chose to participate. The 3 members of the EFTA that have chosen to be members of the EEA are bound by the terms of the Agreement on the EEA which states that any non-EU members must adopt most EU legislation concerning the single market, to obtain access to it. There are however exclusions to the laws it is required to adopt notably on agriculture and fisheries.

3.2.2. Milestone Events in the Creation of the EU

The following section highlights some of the key events that have helped to shape and influence the development of the European Union structure that exists today. This is a broad and complex topic and, as such entering into any great detail or covering every event is outside the scope and limitations of this research project. They are listed to

provide an understanding, albeit at an abstract level, of the foundations of the Institution that produces the legislation under study in this report and how the legislative powers are structured.

Council of Europe and European Court of Human Rights (The Treaty of London)

As inferred previously the end of World War II in 1945 was a catalyst to greater cooperation and closer political union, particularly in Europe where the legacy of military destruction was evident throughout the continent. In 1948, a failed attempt to establish a European Constitution led instead in 1949 to the creation of the Council of Europe (CoE), a protector of human rights and champion of democracy and civil liberties. Not to be confused with the European Council, the CoE is still in existence today and currently has 47 direct member countries and 6 observer states. It does not have any powers to create legislation however it is empowered to enforce some of the special treaties and agreements made between the members. The European Court of Human Rights (ECtHR), established in 1959, is the enforcement body of the CoE and is responsible for monitoring the European Convention on Human Rights (ECHR), one of the key agreements produced by the CoE.

The CoE is an intergovernmental political community that consists of: the Parliamentary Assembly of the Council of Europe (PACE), with over 300 members of parliament from all the CoE member states, who meet four times a year to hold week-long plenary session at its seat in the Palace of Europe in Strasbourg; the Congress of Local and Regional Authorities, with over 600 representatives from leaders of local regions and authorities; and the Committee of Ministers comprising the Foreign Affairs Ministers from each of the member states and their permanent representatives (or deputies). The head of the CoE is the Secretary-General, currently Thorbjørn Jagland (former Prime Minister of Norway).

The creation of the CoE inspired the formation of the EU. It was the first step in the integration of political and social values that the EU would be founded upon and the inter-government and parliamentary structure of the CoE would be replicated in the EU. In 1952 the CoE also created the blue flag with the circle of 12 stars that has commonly been associated with the EU who adopted it as their official emblem in 1983.

North Atlantic Treaty Organisation

1949 was also a pivotal year for military union when the signing of The Washington Treaty by the US, Canada and 10 European countries (currently there are 28 member

countries) reinforced the relationships formed by the allied forces during World War II when they agreed to stand together to promote democracy and peaceful resolution to conflict involving members and neighbouring states.

European Coal and Steel Community (The Treaty of Paris)

The signing of the Treaty of Paris in 1951 by France, Germany, Belgium, Netherlands, Luxembourg and Italy established the European Coal and Steel Community (ECSC) to develop a common trade and production policy on the European continent. This was seen by its proposer, French Foreign Minister Robert Schumann, as an effective way of limiting the possibility of further wars between the signatories, as, amongst other reasons, it would make it difficult to secure the raw materials needed to service a military conflict. In order to set policy and agree production, an assembly of representatives of the industries (then all state-owned) and a separate Council of Ministers were established to ensure power wasn't concentrated in the hands of a few individuals. Along with the CoE, mainly to its governance structure, the ECSC is seen as the political precursor to the EU but has since undergone a dramatic transformation to become the institution it is today.

European Economic Community and EURATOM (The Treaty of Rome)

In 1957 the six members of the ECSC signed The Treaty of Rome, creating the European Economic Community (EEC), a common market to promote free movement of capital and labour and produce a customs' union, and the European Atomic Energy Community (EURATOM) to jointly develop nuclear energy. The two new Communities were created with the same structure as the ECSC with a Council of Ministers and a Parliament made up of representatives from members' national parliaments.

European Court of Justice

A year later in 1958 the European Court of Justice (ECJ) was created to interpret the application of the articles in The Treaty of Rome and rule in disputes over decisions made by the EEC.

European Free Trade Association

In 1960 the UK, Austria, Denmark, Norway, Portugal, Sweden and Switzerland created the European Free Trade Association (EFTA) as an alternative free trading bloc to the EEC. Unlike the EEC however the EFTA did not feel it necessary to set standard trade tariffs for members to trade with non-members or to set up EFTA institutions to set policy or deal with issues that arose.

British Request to Join EEC Vetoed

Britain Denmark and Ireland applied for membership to the EEC in 1961 however Britain's application was vetoed in 1963 by French President Charles de Gaulle who raised concerns that Britain did not seem committed to European integration. He was also concerned over the close relationship Britain had with the US and feared that allowing Britain to join the EEC would diminish post-war France's role in global affairs.

European Communities Commission (The Treaty of Brussels)

The second of two Treaties to be signed in Brussels (the first was a defence treaty, an extension of the Treaty of Dunkirk signed in 1949), and more commonly known and the Merger Treaty, was signed in 1965 and was a significant step towards creating the structure of the EU recognisable today. It combined the separate entities of the ECSC, the EEC and EURATOM in order to create one European Communities Commission (ECC), resulting in a single Council and a Commission to represent all three communities. After a process that took 3 years to complete the ECC customs union was finally completed in 1968.

Accession of UK, Denmark and Ireland to ECC

After the failed attempt to join the EEC, the UK, Denmark, Ireland and Norway signed accession treaties to join the ECC in 1972. Denmark, Ireland and Norway all held national referendums that year; Denmark's and Ireland's citizens voted to join whereas Norway's rejected the treaty. The UK eventually signed its accession in 1975 after holding a successful referendum once it had renegotiated its terms of entry. The European Communities Act was introduced into UK law in 1972 to allow this accession to take place. Section 2 of the Act deals with the incorporation of European Community law into UK law and defines how primacy of this law would be interpreted by UK courts.

The Trevi Network

In 1976 the first meeting of the Ministers of Justice and Interiors of the ECC member states took place in Rome, where the group took its name from, to cooperate on cross border policing and counterterrorism issues.

The European Monetary System

In 1979 all ECC members except the UK signed up to the European Monetary System (EMS) who subsequently introduced the European Currency Unit (the Ecu), which was primarily used as a unit of currency for ECC budgetary affairs. The EMS also created the Exchange Rate Mechanism (ERM) to provide members' national currencies an exchange rate band that was denominated in Ecus.

The Single European Act

Greece, Portugal and Spain joined the ECC during the 1980s, while shortly afterwards Greenland became the first member state (and the only one until the UK's recent vote) to withdraw its membership, after joining alongside Denmark who it was in a political union with at the time. Its biggest concern at the time was the increasing talk of a closer political union between the member states and in 1987 the EU took that further step that Greenland feared, as the Single European Act was adopted, designed to remove a series of trade, capital and labour movement barriers. The Act created a single market that would integrate the ECC further by setting some common political as well as economic objectives and increasing the legislative powers of the ECC Parliament.

The Maastricht Treaty – Treaty on European Union

The Maastricht Treaty on European Union was signed in December 1991 and came into force in 1993, after a difficult passage into law in some member countries, namely Denmark, France, Germany and the UK. It created three legal entities, known as the "pillars", of the European Union (these were eventually merged into one entity in the Lisbon Treaty): the European Communities (EC); the Common Foreign and Security Policy (CFSP); and the Police and Judicial Cooperation in Criminal Matters (PJCCM). This significant Treaty formalised, in Article 13, the governance structure seen today in the EU Institutions. It set out a plan for a monetary union and laid out objectives on social policy that allowed all citizens of EU member states to live in any other EU country. It also triggered greater cooperation on foreign affairs such as national security, asylum and immigration policies and saw the Trevi network transformed into the Justice and Home Affairs Council, although the UK and Ireland negotiated an optional approach to greater levels of control over these areas being passed to the EU. After joining the ERM in 1990 Britain was forced to leave just two years later after market forces moved against the British Pound and devalued it to such a level it threatened to destabilise the process of creating a monetary union. It wasn't surprising when the Euro was adopted shortly afterwards that the UK, along with Denmark, were able to negotiate an opt-out clause of the European Monetary Union (EMU).

European Economic Area

Established in 1994 the European Economic Area (EEA) is the single market of the EU which allows the free movement of persons, goods, services and capital within one internal market. The resulting Agreement of the EEA states that membership of the EEA is open to either member states of EU or the EFTA.

The Treaty of Schengen

As well as seeing three new states join the Union, 1995 also saw the adoption of the Schengen pact to remove internal borders between EU member states on the mainland. This was a move to allow greater movement of people and goods across the Union whilst allowing member's border security forces to focus efforts on controlling external borders. After Ireland adopted the Schengen Treaty two years later when it became EU law, the UK was the only state to keep its opt-out state and whose borders have since remained unchanged, albeit remaining in the Common Travel Area.

The Treaty of Amsterdam

The Amsterdam Treaty, signed into existence in 1997, made substantial changes to the Maastricht treaty as a number of powers were passed to the EU to strengthen laws on employment, discrimination, immigration and asylum and civil and criminal laws. It also formalised the social chapter of the Maastricht Treaty by writing it into EU law.

The Treaty of Nice

Signed into being in 2001 and coming into force in 2003 the Treaty of Nice amended the Treaties of Rome and Maastricht that saw the creation of the ECC and the EU. Its aim was to reform voting structures in order to facilitate the expansion eastwards to new member states. It also created subsidiary courts under the ECJ and the Court of First Instance (now known as the General Court or EGC) to deal with specific areas of law.

Adoption of the Euro

By 2004 national currencies had been replaced and the Euro became the official currency of 12 countries with only Sweden, Denmark and the UK opting out of the monetary union.

EU Constitution

2004 saw the creation of an EU Constitution as ten more countries gained accession to take the total number of members to 25 (bolstered to its current 28 strong member by the accession of Bulgaria and Romania in 2007 and Croatia being the latest to join in 2013. However, efforts to ratify the Constitution were halted by France and the Netherlands whose citizens rejected the plans, throwing the future plans of closer union into question.

The Lisbon Treaty - Treaty on the Functioning of the European Union (TFEU)

Signed in 2007 and coming into force in 2009 The Lisbon Treaty amended the previous Treaties of Rome and Maastricht that established the creation of the European Union. The three legal pillars of the European Union were merged into one legal entity. One of the key amendments to the previous Treaties was the move away from needing

unanimous agreement in Parliament to pass legislation in over 45 different policy areas towards a qualified majority and in some cases a double majority (a 55% majority in Parliament representing over 65% of EU citizens). Parliament's powers were also strengthened by extending the areas governed by ordinary legislation procedures (see Section 3.2.4.2) and by giving MEPs more time to scrutinise and reject legislation proposed by the EU Commission. It also made binding the Charter of Fundamental Rights of the European Union, the successor to the failed EU Constitution, which amongst other things for the first time enshrined in law the jurisdictional relationship between EU legislation and conflicting national laws. Another first was the inclusion in the Treaty of explicit articles to allow member states to leave and re-join if they so wished.

The areas of policing and criminal justice became subject to the powers of the European Commission and the jurisdiction of the CJEU. However, the UK negotiated a general opt-out as provided for under Article 10(1) of Protocol 36 of the Treaty with consent to opt-in to selected measures under Article 10(5). The UK used its powers to opt-out of the general provision but opted-in to 35 of the measures which were enacted into law by the creation of the Criminal Justice and Data Protection (Protocol No 36) Regulation 2014.

Two specific measures relating to data protection that were included in the Protocol 36 Regulation related to two EU Council Decisions (2008/977/JHA and 2006/960/JHA), known collectively and the Framework Decisions, on the processing of personal data in the course of cooperation in police and criminal judicial matters between EU law enforcement authorities and the simplification of the exchange of information and intelligence. These are discussed further in Section 3.2.5.6.

Secession of the UK

Taking advantage of the secession clause in the Lisbon Treaty, the UK held a referendum in 2016 to decide whether to stay in the EU or withdraw. The shockwaves are still being felt globally from the results as the UK citizens made the historic decision to break away from the EU. A long process of disentanglement lies ahead as: laws enacted by the passing of EU legislation not enacted into UK law by the passing of national legislation (see Section 3.2.4) are reviewed; trade agreements are renegotiated; and a new order of cooperation with the EU member states is established. This decision, and the specific impact it will have on the data protection legislation that is the focus of this report is discussed further in Section 7.

3.2.3. EU Institutions

As previously stated there are seven Institutions in the EU; each has a role in establishing laws and providing a stable and standardised environment for the member states to coexist in. The roles of the Institutions have evolved over time and powers have been conferred to each with subsequent Treaties. They are designed to ensure that no one Institution has more power than any other and that each has oversight, in varying degrees, over one of the others.

This section provides an overview of these Institutions and how they work together.

First Institution – European Parliament

The European Parliament consists of over 750 Members of European Parliament (MEPs) MEPs are elected by citizens in each region of each member state by proportional representation for a fixed 5-year term of office, to act on their behalf. Included in the powers given to Parliament by the Treaty of Lisbon, is the approval of the budget set out by the European Commission, which the President of the European Parliament, who is elected by MEPs to serve a 30-month term, signs into being. As well as chairing all the Parliamentary meetings and addressing the Council before each of the Council's meetings, the President of the Parliament, currently Martin Schultz, represents the Parliament in international relations.

The Parliament has 20 permanent committees tasked with conducting the majority of the undertakings of Parliament and scrutinising legislation proposed by the Commission (this process of enacting law is discussed further in Section 3.2.4.2). One such committee is the Civil Liberties, Justice and Home Affairs (LIBE) Committee who *"is responsible for the vast majority of the legislation and democratic oversight of Justice and Home Affairs policies. Whilst doing so, it ensures the full respect of the Charter of Fundamental Rights within the EU, the European Convention on Human Rights and the strengthening of European citizenship."* One of the areas that LIBE is tasked with the oversight of is data protection legislation.

Second Institution – European Council

The European Council comprises the Heads of States and Government (Presidents and Prime Ministers) of all EU member states, the President of the European Commission and the President of the European Council. It is defined in the Treaty of Lisbon, the agreement that forms the basis of the constitution of the EU, as a body that "shall provide the Union with the necessary impetus for its development." (2007). It is the assembly that

determines the political direction of the EU and is thought by many to be the top political institution of the "Tripartite" of EU governance. It is the key legislative body that finalises negotiations on international agreements and decides on policing and judicial measures for the collective. The President of the European Council, currently Donald Tusk, represents the EU collectively at the level of "Heads of States" on foreign and security policies. The President chairs the Council, facilitating consensus amongst members and ensuring the decisions taken are implemented. The President also reports to the European Parliament after each meeting.

Third Institution – The Council of the European Union

The Council of the European Union (often referred to as the Council of Ministers) is an Institution made up of a delegated permanent Minister from each of the member states and is the third of the seven institutions. As well as the Council of the permanent Ministers, there is also a Committee of Ministers comprising the Foreign Affairs Minister from each member state. Working Parties are formed and disbanded as the need arises depending on the area of policy or law under discussion comprising Ministers representing the interests of national governments in the related area. There are 10 different configurations all responsible for oversight and policy formation in different areas. As such who is in attendance at each meeting is contingent on the matter at hand. For example when discussing the data protection legislation the Ministers in the Justice and Home Affairs Committee would be in attendance, which would consist of the Ministers identified by their own governments to represent the member state at EU level in such matters.

The Presidency of the European Council changes every 6 months as it rotates around the different member countries' governments. The Council Presidency works in "trios" comprising the resident Presidency and the next two countries in rotation. The Presidency currently resides with the Slovakian Parliament and its Prime Minister, Robert Fico, is the Leader of the Presidency "trio". The other two countries in the current "trio" are Malta, who will be next in rotation for the Council Presidency, and Malta, who will follow Slovakia. According to the Presidency website (2016) it has two key tasks:

"Planning and chairing meetings in the Council and its preparatory bodies" and "Representing the Council in relations with the other EU institutions".

Fourth Institution – European Commission

This is the European Union's Executive body and it is responsible for drafting proposals for new EU laws, making the decisions about how EU funds are allocated, the implementation of EU-wide policies and ensuring EU laws are enforced across member states. It comprises one representative from each of the member states. It is the only body that has the right to initiate legislation however since the Maastricht Treaty was ratified the European Parliament has the right to ask the Commission to draft a proposal. The Commission also has jurisdiction over matters affecting countries outside of the EU for policies that affect the EU member states and the President of the European Commission, currently Jean-Claude Juncker, represents the EU at "heads of state" level for such matters as trade agreements and international development.

According to the European Commission's own website (EC-Europa 2016) the appointment of the President, the 7 Vice Presidents and the 20 Commissioners that make up the "College of Commissioners" is a complex procedure that starts with the European Council proposing the candidate for President to the European Parliament who then decides by a qualified majority vote.

"Following this election, the President-elect selects the 27 other members of the Commission, on the basis of the suggestions made by Member States. The final list of Commissioners-designate has then to be agreed between the President-elect and the Council. The Commission as a whole needs the Parliament's consent. Prior to this, Commissioners-designate are assessed by the European Parliament committees."

The President of the EU Commission has the power to dismiss Commissioners and/or appoint them to a different portfolio of duties within the Commission.

Fifth Institution – The Court of Justice of the European Union;

The Court of Justice of the European Union (CJEU) is the primary legal Institution of the EU. Originally established in 1952 as the Court of Justice of the European Coal and Steel Communities (CJECSC), it was then renamed in 1958 to become the Court of Justice of the European Communities (CJEC), before being given its current name in 2009 with the passage of the Lisbon Treaty into law. CJEU's primary function is to oversee the implementation and interpretation of the Treaties. This Institution consists of the superior court plus 3 separate courts: the European Court of Justice (ECJ); the General Court (also known as the Court of First Instance); and a court specifically to

resolve employment disputes of EU staff, the Civil Service Tribunal. The function and relationship between these courts is discussed in more detail in Section 3.2.4.3.

Sixth Institution – The European Central Bank

The European Central Bank (ECB) is the main bank for the 19 EU members that have entered into a monetary union (Eurozone members) and have the Euro as their currency. They state on their website that their "main task is to maintain price stability in the Euro area and so preserve the purchasing power of the single currency" (ECB 2016). Another of their functions is to supervise banking activities within the EU, in particular those in the Eurozone. The President is appointed by a majority vote of the Eurozone European Council members for an 8-year non-renewable term of office. The current President of the ECB is Mario Draghi, former Vice Chairman and Managing Director of Goldman Sachs International and Governor of the Bank of Italy.

Seventh Institution – The European Court of Auditors

According to the Europa website (2016), the European Court of Auditors (ECA) is an independent external body that consists of one representative from each member state tasked with looking after "the interests of EU taxpayers." Created in 1975, it is responsible for conducting audits on how EU funds are "raised, spent, achieved value for money and accounted for." It also gives advice on how EU finances can be managed better. Whilst The ECA has no legal powers it is responsible for reporting any suspected fraudulent activity, corruption or other illegal activity, and since the Maastricht Treaty came into force it has the powers to bring an issue to the European Court of Justice. The members to be appointed are selected for their complete independence and expertise of having working in an auditing capacity previously. They are discussed in a Budgetary Control Committee of the EU Parliament and selected members are put forward to be unanimously elected by the Council of European Union for a term of 6 years. The President, currently Vítor Manuel da Silva Caldeira, is elected from one of the members for a 3-year term which can be renewed.

3.2.4. EU Law

There are three key interdependent bodies that make up the EU legislature able to propose and create laws. Each legislative body represents different interest groups and they usually work together to implement new laws. The EU Parliament represents the voice of the EU citizens, the EU Council is the representative of the governments of the member states and the EU Commission represents the interests of the legal entity that is

the EU. The process of introducing and adopting new legislation is quite a complex one which involves for the most part, each of these three Institutions.

3.2.4.1. Types of Legislation

According to EUR-Lex (2010), there are three types of legislation that can be created by the EU: Primary; Secondary; and Supplementary.

Primary Legislation

Primary law comes about by direct negotiation and discussion between EU member states and concerns the legal framework that the EU Institutions operate within. This includes all the EU Treaties previously mentioned including the Treaty on the European Union (Maastricht Treaty), which established the seven Institutions of the EU, and the Treaty on the Functioning of the EU (Rome Treaty), which determines the degree of authority the EU has to pass laws and what the principles of those laws are. In essence, primary law establishes the powers each of the Institutions hold, who each Institution is accountable to and how. As well as the Treaties, primary law also includes any amendments to these Treaties, the Protocols (or rules on how to apply the principles set out in the Treaties) associated with the Treaties, and the accession of new member states to the EU. Treaties are amended to reform the EU, when new member states join, or when powers or responsibilities change.

Secondary Legislation

Secondary legislation is the enactment of policy within the framework set out in the Treaties and according to EUR-Lex comes in the form of either:

- Unilateral Acts; or

  These can be subdivided further according to:

  - those that appear in Article 288 of the Rome Treaty, namely Regulations, Directives, Decisions, and Recommendations; and
  - those that don't, Communications, Recommendations, Opinions, White and Green Papers.

- Agreements.

  These encompass any form of legally binding understanding made between:

  - the EU and a non-EU organisation or country;
  - EU member states; and

- EU Institutions.

Regulations

Regulations are legislative instruments in their own rights and are binding and directly applicable in all EU member states without the need to implement associated legislation nationally. Once agreed there is normally a 2-year adoption period to allow time for procedures and compliance rules in member states to adjust.

Directives

Directives are a set of objectives applicable to all member states but they differ from Regulations in that in order to become legislation each nation state must introduce its own law to meet the objectives. Directives offer authorities in member states some flexibility over how the objectives are achieved and over the means of implementation. Directives with a timetable for implementation; this often allows the member state some time to develop an enacting law then time to transition to the new legislation.

Decisions

Much like a Regulation, a Decision is binding in its entirety but only for its intended recipients. It can be addressed to one, several or all member states, one or several businesses, or one or several business sectors. A Decision can be adopted by legislative procedure as other laws or non-legislative in that it is enacted by powers delegated to the EU Commission by other Institutions or specific clauses in the Treaties. Decisions are taken more commonly when there is a need to implement a policy on a subset of member states or organisations and/or there is insufficient time to follow standard legislative procedure. A Decision enters into force either on the date specified within the Decision or 20 days after it has been published in the Official Journal of the European Union.

Recommendations

According to Europa (2016) a Recommendation is a non-binding instrument that "allows the institutions to make their views known and to suggest a line of action without imposing any legal obligation on those to whom it is addressed."

Opinions

An Opinion is a non-binding instrument that can be issued by the legislative Institutions and Committees, to offer a specific economic or social position on an issue from the perspective of different regions. They are often issued to help provide guidance and stimulate discussion whilst laws are being formulated.

Supplementary Legislation

According to EUR-Lex (2010) Supplementary Legislation "brings together the unwritten sources of European law having judicial origin." This comprises all sources used by the ECJ as rules of law to guide its judgments in cases and bridge the gaps where the primary or secondary legislation are not able to provide adequate guidance. These include public and international laws and general principles of law, or case law, although some fundamental rights long seen as general principles of law are increasingly being enshrined in Treaties thereby becoming elements of primary legislation, the most notable example being the European Convention on Human Rights. This is in a bid to ensure that rules are enforced uniformly across different fields and not open to broad interpretation depending upon the domain and situation it is being applied in.

3.2.4.2. Legislative Process

This section describes the process by which EU legislation come into being. There are two key methods known as the Ordinary Legislative Procedure and the Special Legislative Procedure.

Ordinary legislative procedure

Legislation is usually effected in a process known as Co-decision, recently renamed as the Ordinary Legislative Procedure, which refers to the dual roles that the Parliament and Council take in the law-making. The main objective of introducing law in this way is to allow the citizens of the EU through the MEPs and the national parliaments through the Council of Ministers to have an equal opportunity to contribute to and reach consensus over the resulting legislation.

Proposal Issued

Only the Commission has the power to draft and propose new laws. Under this procedure however in certain circumstances the Parliament or the Council are allowed to request that the Commission consider proposals for Regulations and Directives, though it still remains entirely in the realm of the Commission what form those legal proposals will take. It is also possible for the Commission to act on a Citizens' Initiative to propose legislation but these instances are quite rare.

The Commission issues a legislative text, or proposal for a new law, to the Council and Parliament, as well as to all national parliaments of EU member states. This is preceded by an obligatory Impact Assessment undertaken by the Commission to determine what effect the legislation is likely to have if adopted or, conversely, if not. It also usually

follows a consultation period, initiated by the publication of a Green Paper, which is aimed at stimulating discussion amongst key stakeholders. The results of the consultation process are then set out in a White Paper, which outlines the key legislative points to be covered in the proposal.

National Parliaments' Role

National parliaments have eight weeks from the time the legislative text is issued to raise any concerns. If a minimum of 10 parliaments (or 7 in matters relating to criminal or police cooperation) do not think the legislation meets the principle of subsidiarity as set out in Article 5(3) of the Treaty of Lisbon then it must be reviewed by the Commission who then decides whether to withdraw, amend or keep the proposal as it is.

> *Principle of Subsidiarity*
> "In areas which do not fall within the Union's exclusive competence, the principle of subsidiarity, laid down in the Treaty on European Union, defines the circumstances in which it is preferable for action to be taken by the Union, rather than the Member States." (Fact Sheet Article 5(3) Treaty on the European Union (Europa 2016))

If the number of parliaments that consider the legislation does not meet the subsidiarity clause passes a simple majority (currently 15 out of 28) and the Commission, after review, chooses to maintain it regardless then the Commission must justify its decision to the Council and Parliament. The two Institutions must then come to a decision on the matter before concluding the first reading of the legislation and if either Institution by a simple majority of 55% upholds the national parliaments decision then the legislation is withdrawn.

1st Reading in Parliament

The first reading of the legislation that does meet the subsidiarity clause is the privilege of the EU Parliament. The proposal is passed to the relevant Parliamentary Committee who produces a report on the proposal including any concerns or suggested amendments. Any MEP can propose amendments to legislation and it is not uncommon for a Committee to seek external advice from other EU Institutions, sub-committees and/or experts in a particular field whilst drafting its report. This advice can come in the form of an Opinion, which, as previously stated, is a non-binding legal instrument as such are published in the Official Journal of the European Union along with the resulting Directive, Regulation or Decision. After debating the legislative text on the basis of the

Committee's report in a plenary session, members of Parliament vote to adopt a position to accept, reject, or accept subject to amendments. If amendments are suggested the Committee Report is passed back to the Commission to review the recommendations. There is no time limit for this first reading to be completed.

1st Reading in Council

This position with any suggested amendments is then passed to the Council of Ministers for its first reading. A Working Party is convened and chaired by the representative from the member state currently holding the rotating Presidency.

The Council can choose to ignore, accept or reject the Parliament's position. If the Council position agrees with the position of the Parliament by a qualified majority then the proposal is adopted after the first reading. Whilst not legally bound to take the views of Parliament into account, the Council is however obliged to allow a proposal to have a first reading in Parliament and for Parliament to take a position on it prior to the Council delivering its position, although it can conduct preparatory work on the proposal before then. It may reach an Agreement in Principle before the Parliament has concluded its first reading, in an attempt to encourage consensus of adoption at an early stage, or reach a Political Agreement, which is then refined further before being formally adopted as the first reading position.

If the Parliament accepted the proposal subject to amendments then the Council has to vote on the amendments as well. If the Commission has produced an amended proposal the Council can adopt a position on the amended proposal by majority vote otherwise it must agree unanimously on the proposal and amendments.

The Council position may differ from that of the Commission. Arguably, as it is not written into any Treaty, the Council could choose to reject the proposal outright by a qualified majority. However, in a situation likely to raise a constitutional legal issue such as this it would be more probable that the Commission would withdraw or amend its proposal first.

Of course the Council position may not accord with that of the Parliament, and the Council may wish to suggest its own amendments to the proposed legislation. The text of the first reading position and a Statement of Reasons outlining the discord, are sent to the Parliamentary Committee and the Commission. The Commission may also make a

statement that it issues to Parliament of its thoughts on the Council position and whether it supports or rejects it.

As with the Parliamentary process there is no time limit for the Council to conclude its first reading.

2nd Reading in Parliament

The first reading position of the Council is usually debated at the first plenary session of Parliament that takes place after its adoption.

If a proposal needs a second reading it is common for informal discussions to take place between representatives of the Parliament, Council and the Commission, prior to formally accepting the first reading positon of the Council in the plenary session. The informal discussions aim to expedite a negotiated position of the first readings prior to triggering the start of a 3-month deadline (a possible further 1 month may be agreed if needed) within which a second reading position must be taken by. This time limit starts the day after the Council's first reading position has been debated in the Parliamentary plenary session.

If Parliament accepts the Council's first reading position or fails to reach a position itself within the time limit allowed, the proposal is adopted on the Council's first reading position. Amendments at this stage can be proposed but only in limited circumstances, from specific parties. As with first readings, all second reading amendments must be voted on in Parliament and be passed by a majority. The outcome of this second reading is communicated to the Commission and Council. The Commission issues an opinion on the Parliament's amendments at the second reading, which guides the Council on the voting procedure it needs to adopt, for example the requirement of a unanimous vote to accept an amendment if the Commission opposes it.

It is also possible with a majority vote for Parliament to reject the Council's first reading position outright thereby ending the legislative process, although this is a very rare occurrence.

2nd Reading in Council

As with Parliamentary second readings, the Council also has 3 months (4 if an extension is agreed) to complete its second reading, from the point it receives the official

Parliamentary position. Again, informal discussions are instigated while Parliament is still debating its position with a view to reaching full agreement at the second reading stage. If all amendments in the Parliament's second reading are accepted by the Council in their entirety the proposal is adopted. However, if any or all amendments are rejected a Conciliation Committee is convened within 6 weeks (with the possibility of extending this by a further two weeks) of the Council adopting its second reading position.

Conciliation Committee

The Conciliation Committee comprises equal number of representatives from both Parliament and Council. As well as having to start the process within a 6 week period the Committee also has to conclude proceedings within a further 6 weeks (with the possibility of extending it to 8). Negotiations to reach a compromise position for both parties continue until all amendments are either accepted or there is a failure to reach agreement and the proposal is rejected thereby halting the legislative process.

If a compromise position is reached a joint text is produced, including all the redrafted amendments, which is ultimately presented to both Parliament and the Council for a third and final reading.

3rd Reading in Parliament

At this stage in the process no further amendments are accepted; the joint text must remain unchanged. There is again a window of 6 weeks (or 8 if agreed) by which to conclude the third reading. The joint text is debated and voted on in a Parliamentary plenary session. The joint text is then either accepted by a simple majority vote or rejected if it fails to reach this majority. A rejected joint text would halt the legislative process at this point. If the Parliament accepts the joint text at the third reading it is then passed to the Council for approval.

3rd Reading in Council

As with the Parliament, the Council also have 6 (or 8) weeks to complete the third reading stage. A qualified majority is needed to approve a joint text, anything less and it is rejected thereby halting the process. However, whilst there are several examples of Parliament rejecting a joint text, the Council have so far not done so.

If and when a proposal is adopted, regardless of at what point in the process this is, it is then signed into being by the Presidents and Secretaries-General of the Council and Parliament and is published in the Official Journal of the European Union.

Special Legislative Procedures are used in those circumstances where legislation is deemed to be of such importance as to be crucial to EU member states. Examples of these would be the decision to accept a new member state, foreign policy issues, and the appointment of Commissioners.

Consultation Process

Prior to the Single European Act being adopted most legislation was introduced using the Consultation process.

Under the Consultation Process, legislation is still proposed by the Commission but supremacy lies with the Council. Whilst the Council take the ultimate decision it is bound to consult with Parliament for its opinion; nevertheless it can choose to accept or ignore it. It is not uncommon for the Council to adopt the latter position and has been known to reach agreement before Parliament has given its opinion. However, since the ECJ stepped in and struck down legislation that had been adopted before the Parliament's position had been adopted, the Council waits to communicate its decision.

Consent Process

In the same way as all legislation, decisions to be made under this process originate with a proposal from the Commission. This proposal is then given to Council to adopt a position on. As with the Ordinary Legislative Procedure the consent of Parliament is required in order for the legislation to be adopted. However, unlike the Ordinary Legislative Procedure, the Parliament can only choose to adopt or reject the position of the Council. It has no power to propose amendments; only the Council have the power to do this. It does include the possibility providing interim reports to the Council and of convening a Conciliation Committee, which is where negotiations take place on the content of the proposal if there is dissent on the position of the Council from Parliament. Therefore, whilst it cannot directly introduce amendments, Parliament can withhold its consent to adopt legislation until any concerns are dealt with.

In some special circumstances such as when negotiating some trade agreements, the Council can adopt legislation without needing the consent of Parliament first.

Commission Only Process

The Lisbon Treaty makes provisions for the Commission, in very limited circumstances to create and adopt legislation without requiring the consent or opinion of either the Council

or Parliament. There have been two instances of this happening in the past, the first relating to transparency between companies and member states (Dir. 80/723 [1980] OJ L195/35) and one on competition within the telecommunications sector (Dir. 88/301 [1988] OJ L131/73).

3.2.4.3. Structure of European Court System

This section will discuss each of the courts in existence within the EU in more detail.

Court of Justice of the European Union

Established in its current form under the Lisbon Treaty, the Court of Justice of the European Union (CJEU) is the fifth Institution of the EU and is a legal entity in its own right. It is the umbrella term for the collective judicial body that comprises the three separate EU courts: the Court of Justice; the General Court; and the Civil Service Tribunal.

Seated in Luxembourg, the organisation that is the CJEU supports the functional needs of the three courts. It is responsible for providing all the buildings and infrastructure requirements of three courts, manages all budgetary matters, administers all the human resources tasks for the courts and maintains a significant library of resources for the three courts and the national judicial system to draw upon. It also provides the translation services for the court transcripts, which need to be disseminated in all the languages of the EU, as all rulings become pieces of legislation that can be used by any member state, regardless of what language a case was heard in or documentation was originally written in. The official language of the CJEU is French and all judges deliberations are conducted in this language however a case can be heard in any one of the official languages of the EU; it is usual for an applicant to the court to have the case heard in his/her own language.

The Registrar of the Court of Justice is responsible for managing all of the departments of the CJEU, and reports to the President of the Court of Justice.

Court of Justice

The Court of Justice (ECJ) is the highest court in the EU and has supremacy over all other law courts in the EU member states in all matters relating to questions of European Union law. Article 234 of the Treaty of Rome accords the ECJ with the jurisdiction for ensuring that EU law is interpreted appropriately and applied uniformly across all countries. It works alongside the national judicial systems of the member states to verify

that legislation is being implemented correctly and consistently throughout. A decision of the ECJ is binding and there is no further appeal possible.

The Court consists of 28 judges, one from each member state, and 11 Advocate-Generals, one from each of the 6 key member states (United Kingdom, France, Germany, Spain, Italy and Poland) with the others serving in rotation (alphabetically) from the other member states. The judges and Advocate-Generals are appointed with the accord of national governments, from experts in EU law whose independence has been proven to be beyond doubt, and they each serve a 6-year renewable term. The President serves a renewable term of three years and is elected by the judges from within their ranks. The current President is Baron Koen Lenaerts, a Professor of EU Law from Belgium. He is responsible for presiding over hearings and deliberations and he is ultimately responsible for the administration of the CJEU as well as for providing leadership on judicial matters in his capacity as a President of an EU Institution.

Types of Cases

According to the Europa website (2016), the key types of cases the Court of Justice deal with are:

- Interpreting the law (preliminary rulings)

  If a national court, in the case of the UK this can be a Magistrates Court or a Crown Court has an interpretation question over a point of EU law or its compatibility with national legislation, and it is unable to pass a judgement without obtaining a clearer analysis of the point raised it can refer it to the ECJ for a preliminary ruling. The ECJ does not deal with appeals on decisions made in national courts, only on points of EU law. When the ECJ has delivered a decision national courts throughout the EU member states must then use the ECJ's interpretation of the point of law in its own rulings of cases.

- Enforcing the law (infringement proceedings)

  If an EU member state's government is seen to be in breach of an EU law, Treaty or fundamental right, the EU Commission or another member state can start infringement proceedings against it. If the ECJ rules that the member state is in fact failing to comply and the member state subsequently does not attempt to rectify the

problem then a second case may be brought against it that could result in a monetary fine.

- Annulling EU legal acts (actions for annulment)

  If a member state or one of the EU Institutions considers that a piece of EU legislation is considered to be contravening the fundamental rights of individuals or violating an EU Treaty it can ask the ECJ to annul the Act. Citizens also have the right to bring annulment cases to the ECJ.

- Ensuring the EU takes action (actions for failure to act)

  If an EU Institution is expected to take action on a matter and it fails to do so, other Institutions, member states, and in some cases organisations and citizens are able lodge a complaint with the Court.

- Sanctioning EU institutions (actions for damages)

  If an organisation or a citizen believes that they have suffered through an action or, as in the above point, inaction of any EU Institution or its employees a claim for damages can be brought against it through the ECJ.

Procedure

One judge (known as the judge-rapporteur) presides over a case and one Advocate-General is assigned to each case. There is usually more than one judge examining a case depending on how important and/or complicated the case is likely to be. The judges' panels are usually made up of odd numbers to ensure there can be no tied decisions; most commonly there will be 5 judges but in very rare cases all judges will be in attendance.

There are two stages to a proceeding; a written statement followed, if deemed necessary, by a public hearing. During the written statement stage all witnesses submit their evidence, which is then summarised by the judge-rapporteur and presented at a general meeting of the court where it is decided if a public hearing is necessary and if so how many judges will sit on the panel. They also decide at this stage whether an Opinion is required from the Advocate-General.

If a case progresses to a public hearing it is the role of the Advocate-General to ask questions of the lawyers representing all parties and to provide an Opinion after the hearing if one has been requested by the judges. Judges deliver their verdict once they have received any Opinions and deliberated over the case. The Opinions of the Advocate-Generals are not legally binding but are known to influence the judges' decisions (Europa Rules of Procedures 2012).

General Court or Court of First Instance

The General Court (or Court of First Instance as it was previously known) like the ECJ is made up of 28 elected judges one from each member state, who serve 6-year renewable terms of office. They also elect a President from within their ranks for a 3-year renewable term, currently Marc Jaeger, a Judge from Luxembourg.

The procedure followed by the General Court is very similar to that of the ECJ however cases can be heard by one judge and are usually heard by a panel of no more than three judges, unless the case is deemed to be substantially complex or may have far-reaching consequences for member states when all judges may be in attendance. There are no Advocate-Generals involved in the proceedings of the General Court but the Judge-Rapporteur can act in this capacity if required.

An individual or a member state that believes its rights have been violated or has a complaint that falls within the jurisdiction of EU law has the right to make an application to the General Court rather than a national court. The application is initially made in writing and the court contacts the other party in the case to submit its defence. The points of the case are written up and published as a Notice in the Official Journal of the European Union to allow any other parties that may have something of interest to contribute to the case to intervene and submit evidence to the court. Again, as with the ECJ proceedings, the written stage may not be sufficient to reach a decision. Consequently the case may require an oral stage where lawyers representing applicants and defendants can present evidence in person and presiding judges can query it directly.

The European Court of Human Rights

The European Court of Human Rights (ECtHR) is open to the member states of the CoE, hence all signatories to the European Convention of Human Rights (ECHR), and by default, given that all EU members are also all members of the CoE this includes member states of the EU.

Based in Strasbourg, the ECtHR was established in 1959 to hear cases arising from allegations of the violation of the ECHR involving any of the adherent countries. Article 34 of the Convention states that "any person, non-governmental organisation or group of individuals claiming to be a victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the protocols thereto" can make an application to the Court.

It wasn't until a half a century later that the Convention was enshrined in UK law by way of The Human Rights Act (1998) thereby providing a direct recourse in UK courts for individuals to refer allegations to of violation of their human rights. Prior to this anyone wishing to bring a case to court had to make an application to the ECtHR. Now, a case must first be heard in the UK and can only be referred to the ECtHR to appeal a decision from the Supreme Court, once all domestic appeals processes have been exhausted.

Whilst all EU member states are signatories to the ECHR and thereby bound by the decisions of the ECtHR, the EU, as a legal entity in its own right, has decided not to sign up to the ECHR and as such does not recognise any supremacy in law of the decisions of the ECtHR. This does cause a possible conflict as the ECtHR will not accept a defence from an EU member state it deems in violation of the ECtHR that the alleged violation was brought about by the implementation of EU legislation. In an attempt to ensure that conflicts in this area do not arise the ECJ give special significance to the ECHR in its rulings.

The ECtHR comprising 47 judges, one from each of the member states, who are elected for a non-renewable term of 9 years at a plenary session of the Parliamentary Assembly of the Council of Europe by a simple majority.

3.2.5. Data Protection Legislation in the EU

Shaped by the United Nation's International Declaration of Human Rights (1948), the notion of cementing the right of privacy into the policies of the governments of Europe originally manifested in Article 8 of the predecessor to the ECHR, the Convention for the Protection of Human Rights and Fundamental Freedoms, created in 1950 by the CoE.

> *"Article 8 – Right to respect for private and family life*

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The Charter was an improvement on the Declaration's Article 12 statement that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence", which is quite vague and broad in its definition. However, rather than being an absolute right, it is a qualified one in that it still allows for some interference; the state has the right under certain circumstances to interfere with this privacy if for example it is deemed necessary to protect democracy, prevent crime or to prevent the rights of others being infringed upon. The fact that there are caveats to the right for privacy has been the topic of many ethical debates and calls for greater qualification of what is meant by the broad terms used. The protection of morals is an example that raises a fundamental question of what is to be deemed immoral, particularly in progressive and democratic societies that are promoting tolerance of others and freedom of speech and expression? And just who should be the authority on this in a community comprising a variety of religious and non-religious beliefs, views on sexuality, and significant cultural differences?

Several factors, over the next couple of decades, brought about the realisation that the protections afforded under Article 8 of the Convention were not extensive enough to safeguard an individual's privacy. The cold war era and the rise of McCarthyism in the US exposed the increasing possibilities for individuals to be monitored much more closely by governments and private companies alike than had been previously supposed. This increased atmosphere of suspicion in the offending countries left the Europeans, many of whom had only recently emerged from a culture of suspicion and repression during the Nazi regime of WWII, feeling vulnerable. Another issue that has grown in importance in the last 60 years is that of the exponential growth in the amount of personal data and private correspondence in existence. This due to the rise of the

computer and the invention of the Internet significantly increased the opportunity to violate this right and was a chief influence on the subsequent development of data protection legislation globally. Another key development of the second half of the 20th century that has contributed massively to the need to create further laws to protect personal data is globalisation and the emergence of extremely large multi-national conglomerates. These super companies with enormous wealth, hence power, have taken advantage of deregulation and greater cooperation between governments to access data, transfer it across borders and make it easily available to others, without oversight. Those particularly within the knowledge industry that commoditise and trade in information and data pose a clear and specific threat to individual privacy.

3.2.5.1. Convention 108

The first piece of European legislation that was specifically aimed at protecting the personal data of individuals was Convention 108 of the Council of Europe, more accurately titled the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, introduced in Strasbourg in 1981. This was preceded and influenced by the introduction of the first pieces of national data protection legislation by European states, a German State law in 1971, a national law in Sweden in 1972 and one in France in 1978. The US was also a lead player in the development of legislation to protect data by producing principles on the fair processing of information in 1973 that influenced global debate and led to the adoption of the Privacy Act in the US in 1974.

The CoE website (2016) states that the aim of Convention 108 is to protect individuals "against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier [sic] flow of personal data."

The Convention defined what was meant by personal data "any information relating to an identified or identifiable individual", a definition that is still applied in current legislation. In fact many of the concepts and protections outlined in the Convention are still evident in the current, and proposed legislation, including the introduction of specific measures for dealing with "sensitive" data in recognition that certain data can leave individuals very vulnerable if mismanaged, misused or disclosed unnecessarily. It also introduced the concept of a controller of data and imposed certain responsibilities on the controller to safeguard the interests of the individual data subjects. The key founding principle of protecting data without restricting its use or suppressing the development and use of technologies that facilitate that use was developed by restricting the conditions

under which data could be collected and stored. The Convention decreed that all data had to be:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored;
- adequate, relevant and not excessive in relation to the purposes for which they are stored; and
- accurate and, where necessary, kept up to date.

It also calls for there to be adequate security measures in place to safeguard the data against accidental loss or theft, for there to be a right for data subjects to have access to copies of any data held on them and the right for data to be amended or erased if it is incorrectly or illegally processed.

A theme central to all legislation specifically aimed at protecting the data of individuals is the need for the individual to have some control over the processing of his/her data and to have the ability to consent to data being used for reasons other than those originally intended and to limit the ability of organisations and governments with access to an increased amount of personal data to interfere unduly with the privacy of a data subject.

3.2.5.2. Data Protection Directive 95/46/EC

Directive 95/46/EC ("Data Protection Directive") is the central piece of EU legislation dealing with the processing of personal data and its cross border transfer. Whilst many EU member states had implemented data protection legislation nationally the level of protection offered varied from state to state, which led to inequality across the EU for data subjects. The development of different rules and regulations in different countries also impeded organisations that wished to operate on a European level and offer services to data subjects in different countries. Despite the development of technologies that could facilitate cross border enterprise, having to navigate and comply with different laws proved to be a very complicated and expensive hindrance to one of the fundamental objectives of the EU, the development of the single market with a free flow of people, products and services.

The creation of a common legislative framework for EU members to work with meant that for the first time there would be an acceptable minimum level of protection afforded to all EU citizens and standards introduced for businesses within the EU or working with companies within the EU to adhere to, without unnecessary operating restrictions being placed upon them. EU member states had two years to create and implement legislation nationally that would meet the objectives set out in this framework law.

The Data Protection Directive uses very similar terminology and principles as those set out in Convention 108. It uses the same definitions of personal and sensitive data, sets out the need for legitimate reasons for processing and the principles to adhere to for data retention, security and adequacy. It goes further however in defining what constitutes legitimacy by setting out specific criteria for processing of both data and sensitive data, including the need for unambiguous consent outside of these lawful reasons. The Data Protection Directive also places the onus on the data controller to provide information on how personal data is going to be processed if it is not explicit in the reason for its collection.

Article 29 Working Party

The Data Protection Directive also established the need for a supervisory authority to oversee the implementation of the legislation and to ensure abuses dealt with consistently across member states as much as national legislation would allow. Article 29 of the Data Protection Directive called for the creation of a Working Party comprising the heads of the supervisory authorities from each EU member states Data Protection Authorities plus a member of the EU Commission. The "Article 29 Working Party", as the group is known, is a highly influential group who meet to discuss current thinking and interpretation of cases passed through EU courts, and debate Commissioners views. It issues occasional "Opinion" documents – the content of which, whilst not law per se, are usually of great interest to practitioners since it represents the current thinking of the countries collectively.

3.2.5.3. European Union Charter of Fundamental Rights

Whilst it was widely recognised that protecting personal data is one of the ways that an individual's private life can be respected and prior agreements had already enshrined this in the value system of the European countries, it was deemed important enough to safeguard on its own merits. The CoE's Convention on Human Rights, as with its UN predecessor combined the right to privacy and the right of having one's personal data

protected under the same Article. When the EU Charter of Fundamental Rights was introduced in 2000 the right to the protection of data was made much more explicit.

Article 7 and 8 of the EU Charter are defined as follows:

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Whilst separating the two rights in this way elevated the importance of data protection it also led to issues of interpretation of the distinction between the two in later rulings.

3.2.5.4. The US Adequacy Decision (Safe Harbor Agreement)

The eighth principle of the Data Protection Directive states that no data shall be transferred to a third country without there being one of three conditions being met: the country has adequate data protection laws in place; the data subject consents to the transfer of data to that country; Binding Corporate Rules are in place; or the company uses authorised standard contractual clauses for data protection.

In order to overcome complex legislation in the US that many deemed to be inadequate for protecting the data of EU citizens and ineffective for those who felt their rights were being breached, the EU and US authorities entered into an agreement to allow

companies that were willing to agree to adhere to a strict set of principles to process the data of EU citizens legitimately. This was published in the US Adequacy Decision 2000/520/EC, known as the Safe Harbor Agreement. Those organisations could be a signatory to the "Safe Harbor" agreement, a self-certification process whereby companies undertake to follow 7 key principles:

1. Notice
   Data subjects must be notified that their data is being collected and how it will be processed. The company should also provide data subjects with details of how to raise a complaint.
2. Choice
   Data subjects must be able to opt out of the collection and processing of their data. Further consent should be sought if the data are to be used for reasons other than those intended on collection and again given the chance to opt out.
3. Onward Transfer
   The company should also be informed of any disclosure to 3rd party regardless of whether it is inside or outside the US and only transfer data to those organisations with adequate data protection measures in place, either another Safe Harbor company or to a company of the Safe Countries list (see Section 4.5.8 for more on this).
4. Security
   Reasonable precautions should be taken to secure data from theft, loss, unintended destruction or disclosure.
5. Data Integrity
   Data should be accurate and adequate to fulfil the intended purpose of its collection.
6. Access
   Data subjects should be allowed access to information held about them and have it amended or deleted if it is inaccurate.
7. Enforcement
   Safe Harbor companies must implement effective measures of recourse to individuals in the event of a breach. Adherence to Safe Harbor is overseen by the US Department of Commerce, allowing for fines of up to $16,000 per day for serious breaches.

The integrity of the Safe Harbor agreement has been brought into question on a number of occasions and studies, including one by an Australian organisation Galexia (2008) who

published a damning report on the scheme, state that self-certification without rigorous enforcement is open to and was being abused. The Galexia report stated that less than a quarter of the +1,500 organisations on the Safe Harbor list provided even the most basic of protection and around 500 either don't exist anymore or did not renew their certification. More worryingly is the finding that more than 200 companies state they have "Safe Harbor" status when in fact they don't. Whilst there have been cases of enforcement, they are few and far between and the high number of abuses of the system have all contributed to devaluing the protection it offers. Galexia recommended strongly that the EU review the agreement and renegotiate a new one. This decision was forced on the EU after the ECJ found that the agreement was inadequate. Details of this case are discussed in Section 4.10.4 and more on the Safe Harbor scheme can be found in Sections 4.5.8.1.

3.2.5.5. Electronic Privacy Directives and Regulations

Directives 2002/58/EC and 2009/136/EC

Commonly referred to as the "ePrivacy Directives", Directive 2002/58/EC and Directive 2009/136/EC legislation specifically related to the processing of personal data and the protection of privacy in the electronic communications sectors. They dealt primarily with personal data traffic that is generated electronically and regulated areas relating to the use and retention of information for marketing purposes and restrictions on data that is collected through websites. Directive 2009/136/EC is more commonly known as the "Cookie Law" and sets the parameters for the use of tracking software on websites. Any company that wishes to place a "cookie" file on a website user's computer is obliged to inform the individual of the intention to do this once they land on the website, and obtain consent to do so before placing the file on the computer. A "cookie" is a small file that interacts with the website to either track which pages that person visits, or to provide quicker access to specific areas of a website for returning visitors.

Privacy and Electronic Communications (EC Directive) Regulations 2003 and 2011

The amount of electronic data being generated began to grow exponentially at the turn of the Millennium as did the number of websites in existence. The ePrivacy Directives were each enacted by subsequent Regulations in order to ensure they were implemented swiftly and uniformly across each member state. The Privacy and Electronic Communications (EC Directive) Regulations 2003 replaced Directive 2002/58/EC and

accordingly The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 enabled Directive 2009/136/EC.

3.2.5.6. Police and Judicial Cooperation in Criminal Matters

While the Privacy Directives and Regulations concern the personal information processed by businesses, the Council Framework Decision 2008/977/JHA is focused on the protection of personal data processed during the co-operation in criminal matters between police and judicial services across the member states. Although the data protection legislation still applied and law enforcement was still expected to adhere to the ECHR in regards to how it processes data, this Decision provided the legal guidelines for sharing data between the various law enforcement and customs authorities, in particular their acquisition, retention and permissible uses.

3.2.5.7. Forthcoming Data Protection Reforms

The ratification of the Lisbon Treaty had its own impact on data protection legislation in two key ways. Article 6(1) strengthened the Charter on Human Rights raising it to the same level as the Treaties. Article 16(1) and 16(2) also explicitly mentions the right for personal data to be protected and for laws to be created that promote the free movement of data thereby elevating some of the key points in the Directive to the level of primary law.

Since 2012 the data protection legislation in the EU has been under reform. 2016 sees the introduction of three key pieces of legislation in this area and these will be covered in differing degrees of detail during the coming sections of this report.

EU General Data Protection Regulation (2016/679)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) is the new legislation to reform the current data protection legislation. This will be covered in much more detail is Section 5.

Criminal Law Enforcement Data Protection Directive (2016/680)

Whilst outside the scope of this report to cover this in detail, it is the second piece of legislation out of the three major data protection reform laws to be introduced in 2016. The official title of the law is the *Directive (EU) 2016/680 of the European Parliament and*

ot the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. As the title suggests it replaces the previous guidelines to police and other law enforcement agencies on how they are able to process personal data. As it is a Directive member states will need to implement national legislation in order to enact the Directive.

Passenger Name Record Directive (2016/681)

Again, the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, is outside the scope of this research however in general this legislation will allow EU member states to share travel data. All member states will be required to pass ticket, itinerary and payment information of anyone coming into or leaving the EU to their newly created, dedicated Passenger Information Units, who will coordinate the data across the EU. In some circumstances it may also be relevant to share data of inter-EU travellers. This legislation is hoped to facilitate the ability to fight criminal activity in a number of areas of growing concern as terrorism, organised crime and people trafficking.

3.3. Local Data Protection Landscape

Based clearly on the principles laid out in Convention 108 the first piece of data protection legislation to be passed in the UK was the Data Protection Act 1984. It cemented in law the 8 data principles that are still in existence in today's legislation. This was subsequently replaced by the Data Protection Act 1998, which brought into force the EU Data Protection Directive 95/46/EC nationally.

The Data Protection Act 1998 is explained in detail in Section 4.

4. Data Protection Act 1998

The Data Protection Act 1998 was passed to give effect to the EC Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data by data controllers and on the free movement of such data) and came into force in the UK in March 2000.

The DPA is based on 8 principles as set out in Schedule 1, Part 2. These will be discussed in more detail further in the section.

Personal information must:

1. be fairly and lawfully processed;
2. be processed for limited purposes;
3. be adequate, relevant and not excessive;
4. be accurate and up to date;
5. not be kept for longer than is necessary;
6. be processed in line with the data subjects' rights;
7. be secure; and
8. not be transferred to other countries without adequate protection.

4.1. Definition of "Processing"

According to Section 1 of the DPA,

> ""processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
>
> a) organisation, adaptation or alteration of the information or data,
> b) retrieval, consultation or use of the information or data,
> c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
> d) alignment, combination, blocking, erasure or destruction of the information or data"

In effect this is any use that personal data may be put to, including but not limited to:

- obtaining and retrieving
- holding and storing

- making available to others within or outside the organisation (including sending by email)
- printing, sorting, matching, comparing, transforming or destroying.

4.2. Definition of "Data Subject"

A data subject is the individual that the personal data refers to. Following are examples of who can be defined as a data subjects:

- Employees
- Past employees
- Prospective employees (job applicants)
- Customers
- Prospective customers (marketing database subjects)
- Agency staff
- Contractors
- Suppliers
- Students
- Citizens/residents/voters

4.3. Definition of "Data Controller" and "Data Processor"

According to Section 1 of the DPA:

> "A "data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;"

This is in contrast to a "data processor" of personal data:

> "A "data processor" means any person (other than an employee of the data controller) who processes the data on behalf of the data controller."

A Data Controller is the organisation that uses the data being processed for its own means whereas a Data Processor only processes the data for use by the Data Controller. An example of this would be the outsourcing of the payroll function within an organisation, whereby the organisation outsourcing the function of its payroll is deemed the Data Controller and the organisation that completes the payroll function is the Data Processor acting on behalf of the Data Controller. The Data Processor must not use the personal

data of the employees of the Data Controller for its own ends and must only process the data in order to complete the function for the Data Controller.

4.4. Definition of "Personal Data"

Personal data is defined as

> "data which relate to a living individual who can be identified…
>
> (a) from those data, or
>
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
>
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

The key elements of this definition are "***data***" which "***relate to a living individual*** who can be ***identified***" (i.e., "***personal***").

4.4.1. Meaning of "Data"

"Data" falls into five categories:

a) All information processed electronically (referred to in the DPA as "information processed by equipment operating automatically in response to instructions given for that purpose").
b) Paper and other manual records intended to be processed electronically.
c) Paper and other manual records in a "relevant filing system".
d) Accessible records.
e) Unstructured manual data held by public authorities.

All information that is held on a computer or on other electronic systems, such as a mobile phone or storage device, will be caught by this definition. However, paper and other manual records are included to a more limited extent, depending on the type of organisation holding the data.

Paper and other manual records

To be included within the DPA, the paper-based or other manual data held by all organisations must:

- be recorded with the intention that it will be processed electronically (for example information collected on paper and subsequently scanned or typed in to a computer); or

- form part of a relevant filing system.

Definition of a "relevant filing system"

The definition of a relevant filing system appears in Section 1 of the DPA:

> *"any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criterial relating to individuals, in such a way that specific information relating to a particular individual is readily accessible."*

This may capture, for example, manual data kept in structured personnel files, card indexes and microfiches.

During the Subject Access Request case of Durant vs Financial Services Authority the Court of Appeal gave a very narrow interpretation to the term "relevant filing system":

> "1) in which the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it under section 7 is held within the system and, if so, in which file or files it is held; and
> 2) which has, as part of its own structure or referencing mechanism, a sufficiently sophisticated and detailed means of readily indicating whether and where it an individual file or files specific criteria or information about the applicant can be readily located."

The ICO Guidance following the Durant case clarifies that to be a relevant filing system, the content of the manual records must either:

- contain only a single category of information (about an individual's complaint, or his account, or his personnel records); or
- be indexed or sub-divided to allow ready access to specific information about a particular individual.

If information within files is stored in random or even chronological order regardless of subject matter, this would not amount to a relevant filing system as the searcher would have to leaf through the file to find specific information about an individual. If the files

were, however, indexed or sub-divided into categories enabling quick access to specific information about an individual, then they will most likely constitute a "relevant filing system".

The ICO suggest applying the "temp test" to determine whether any such filing system is "relevant", i.e., a reasonably competent temporary administrative assistant having been given a short induction or explanation would be able to extract specific information about an individual from a set of manual records without any particular knowledge of the type of work or documents held.

Paper (and other manual) records – accessible records and public authorities

Paper records that form part of an "accessible record" are also caught by the DPA. This captures certain health records, educational records and local authority housing or social services records which were the subject of access rights which pre-existing the DPA.

Paper records containing personal data and held by a public authority (and not falling within a relevant filing system or comprising an accessible record) are also covered by the DPA, but only to a very limited extend (including in relation to subject access requests). This category (known as "unstructured" personal data held by public authorities) was introduced to operate alongside the Freedom of Information Act 2000 (see section on ***Secondary and Related Legislation*** below for more on this).

4.4.2. Meaning of "Personal"

Data will be "personal" if it "relates to" a "living individual" who can be "identified". Each of these elements can be considered separately.

Living individual

The information must relate to an individual, rather than a company or other corporate entity. However, the processing of, for example, the contact details of individuals within a company could be covered. The individual must also be living; information about a deceased individual is not personal data of that individual. However, it could still constitute personal data relating to a relative or other living individual.

Identification

The individual must be capable of being identified from the data in question or from those data and other information that is in the possession of (or likely to come into the possession of) the data controller.

This means that information about an individual that is anonymous will not be personal data, if the data controller does not possess and is not likely to acquire the information necessary to enable it to identify the relevant individual.

Relates to

According to the Durant Court of Appeal case, personal data is data that "relate to" the individual in a way that might affect his privacy – whether in his personal or family life, his business life or in a professional capacity. Personal data must also have the data subject as its focus and be information of a biographical nature (i.e. it would be information that goes beyond the recording of the data subject's involvement in a matter or an event that has no personal connotations or breach of privacy).

However, the ICO and an EC Article 29 Working Party Opinion have taken a broader view on the interpretation of "relate to". Further, a recent ruling, Edem v The Information Commissioner, suggested the Durant "biographical" test should only be applied in borderline cases, where it is not clear whether data are personal or not.

In ICO guidance, "Determining what is personal data", the following approach is suggested. Data will "relate to" an individual in the following situations:

- the data are ***obviously about*** an individual, e.g., a medical history, a criminal record, or a record of a particular individual's performance at work or in a sporting activity; or
- the data are processed to ***learn, record or decide*** something about an individual (e.g., a record about an individual which has been processed in order to obtain information about him, such as his home region or age) or the processing could result in something being learnt or recorded about the individual or otherwise have an impact on or affect an individual. The ICO goes on to give examples of when this may be the case, where the data:
    - are ***linked to*** an individual so as to provide particular information about that person;
    - are being used to ***inform or influence actions or decisions affecting*** an individual; have ***biographical significance*** in relation to the individual;
    - ***focus*** or concentrate on the individual as the central theme; or
    - ***have an impact*** upon an individual when processed (whether in a personal, family, business or professional capacity).

4.5. 8 Principles

The section provides an overview of the eight principles defined in the DPA.

4.5.1. First Principle

Principle 1 of the DPA relates specifically to the processing of the data.

"Personal data shall be processed fairly and lawfully and, in particular, 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."

In essence this means the organisation must have valid and proportional reason for collecting and using personal data.

- have legitimate grounds for collecting and using the personal data;
- not use it in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how it intends to use the data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure you do not do anything unlawful with it such as sell it or share it with others without permission.

4.5.1.1. Schedule 2 Conditions

Under the First Principle, personal data must generally not be process unless one of the following legitimising conditions applies to each and every processing operation:

Schedule 2 Conditions

1. The data subject has given his/her consent to the processing.
2. The processing is necessary:
    a. for the performance of a contract to which the data subject is a part; or
    b. for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary:
    a. for the administration of justice;
    b. for the exercise of any functions conferred on any person by or under any enactment;
    c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
    d. for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Consent

There is no definition of consent in the DPA. Article 2 of the Data Protection Directive states that it means:

> "...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Consent is often obtained by using opt-in and opt-out clauses, but there is no requirement to do it that way. Consent can be orally obtained. Consent can also usually be withdrawn by the individual at any time.

Contractual Necessity

Examples include using a data subject's name and address for the delivery of items bought by the data subject, and using an employee's bank account details to pay salary in.

Legal Obligation

Processing in furtherance of any statutory or other legal obligations imposed on the data controller will be legitimised where the processing is necessary to comply with that obligation.

Vital Interests

The word vital is likely to be construed narrowly due to the reference in Recital 31 of the Data Protection Directive, which refers to the protection of any interest that is "essential for the data subject's life". An emergency medical situation would therefore be covered. It is possible that "vital interests", in addition to serious medical or health issues, could extend to the circumstances involving serious and substantial damage to an individual's property.

Public Functions

This condition covers certain processing undertaken by public sector data controllers and is commonly used to legitimise processing which is carried out under a discretionary power.

Legitimate Interests

There needs to be a legitimate interest of the data controller, and that legitimate interest must not be outweighed by the privacy expectations of the relevant individual.

4.5.1.2. Schedule 3 Conditions

The term "sensitive personal data" is defined in Section 2 of the DPA as personal data consisting of information as to one or more of the matters listed below:

a) the racial or ethnic origin of the data subject;
b) his political opinions;
c) his religious beliefs or other beliefs of a similar nature;
d) whether he is a member of a trade union;
e) his physical or mental health or condition;
f) his sexual life;
g) the commission or alleged commission by him of any offence;
h) proceedings for the commission or alleged commission of any offence.

There are 19 conditions for the lawful processing of sensitive personal data (as set out in Schedule 3 of the DPA and in secondary legislation). Many are esoteric and rarely applicable.

- Explicit consent of the data subject
- Compliance with employment law obligations
- Vital interests of the data subject
- Processing by not-for-profit organisations (political, philosophical, religious or trade union purposes only)
- Information made public by the data subject, e.g., voting habits of MPs (for lobbying purposes)
- Legal advice and establishing or defending legal rights
- Public functions (administration of justice, etc.)
- Fraud prevention
- Medical purposes

The following conditions are UK specific. They appear in the DPA but are not specified in the Directive.

- Records on racial equality
- Detection of unlawful activity
- Protection of the public
- Public interest disclosure
- Confidential counselling
- Certain data relating to pensions
- Religion and health data for equality of treatment monitoring
- Legitimate political activities
- Research activities that are in the substantial public interest
- Police processing
- Processing by Elected Representatives
- Information on offences involving indecent photographs of children regarding payment cards
- Processing of information about a prisoner for the purpose of informing a Member of Parliament about the prisoner and arrangements for the prisoner's release

Under the First Principle using sensitive personal data without one of the above reasons is generally unlawful. If organisations are unable to bring a type of sensitive personal data processing within one of the conditions then processing should either cease or be altered such that it fits within one of the conditions.

Sickness and injury records will usually constitute "sensitive personal data". According to the June 2005 version of the Employment Code such records should, where possible, be kept separate from other records – e.g., records relating to the fact that a worker is absent and the length of absence should be kept separately from records relating to the reason for the absence.

In order to meet the Seventh Principle of the DPA, regarding data security, access to sensitive personal data should be restricted to those members of staff that specifically require such access to carry out their functions and who have received appropriate training in data protection law and practice.

4.5.1.3. Direct Marketing

Direct marketing (i.e., using personal data to contact individuals regarding the activities, products and/or services of an organisation) involves the processing of personal data – e.g., someone's name and address and/or email address.

Organisations must comply with:

- the DPA in relation to all direct marketing communications sent by any media (including post, telephone or electronically). This includes satisfying one of the legitimising conditions for processing and giving data subjects the right to require the data controller to cease direct marketing; and
- the PECR in relation to unsolicited direct marketing communications sent by telephone, fax, email, SMS or other electronic media. As well as covering communications to individual subscribers, the PECR also restrict the sending of unsolicited direct marketing communications to corporate subscribers. An introduction to the rules in relation to email marketing is set out below.

Opt-outs and Opt-Ins

Opt-out or opt-in clauses are often used in relation to direct marketing communications. An organisation will need to assess the circumstances to determine whether an opt-in

and/or opt-out may be appropriate, including the method of communication, whether consent is required under the DPA or PECR, and the general approach which the organisation wishes to take.

Marketing - Email

The PECR require that consent be obtained prior to conducting all relevant email marketing to individual subscribers (e.g. emails to customers or potential customers informing them of the organisation's products/services) except where ***all three*** of the following apply:

1. the sender obtained the details from the intended recipient in the context of a sale or negotiations for the sale of a product or service; and
2. the marketing relates to the sender's own similar/products services; and
3. the recipient is given a simple means of refusing the communications (by an opt-out or otherwise) at data collection and on each subsequent communication.

Therefore data controllers engaging in email marketing campaigns will wish to utilise the above 3-part exception (known as the "soft opt-in") wherever possible. The requirement to obtain opt-in permission under the PECR applies only to emails sent to individuals, not to corporate subscribers.

These rules effectively render the email list rental business unlawful in most cases - thus organisation should buy lists of email addresses for marketing purposes only in exceptional circumstances and only where taking clear warranties concerning the legality of their use for marketing purposes.

4.5.2. Second Principle

The Second Principle provides that personal data must be obtained only for one or more specified and lawful purposes.

The first part of the Second Principle effectively requires that the purposes must be specified. Purposes can be specified in the ICO's register of data controllers and/or in the data controller's fair processing notice.

The second requirement of the Second Principle is that personal data must not be processed in a manner incompatible with the purposes for which they were obtained. Since a different purpose would not necessarily be an incompatible purpose, the Second

Principle does not itself necessarily prevent processing for a purpose other than those specified.

In April 2013 an Opinion of the Article 29 Working Party (WP203) set out extensive guidance for data controllers on the Second Data Protection principle, also known as the "purpose limitation" principle. The Opinion stated that all relevant circumstances must be taken into account when making an assessment of whether further processing is compatible. In particular, the following key factors should be considered:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects; and
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

4.5.3. Third Principle

The Third Principle essentially obliges data controllers to obtain and use only those pieces of information that are necessary for the data controller's purposes for processing such information. In order to pass the "adequacy" test, organisations should hold enough of the right type of information on an individual so as to avoid any decision being made about them to be inadvertently affected by this. In practice, organisations are more likely to breach the "relevant" and "excessive" aspects of the Principle than they are the "adequacy" aspect, since organisations tend to collect too much information on people rather than too little.

Determining whether an organisation is in compliance with this Principle consists of two key steps. The first step is to ascertain the relevant purpose or purposes for processing. The second step is to consider whether each proposed processing activity is actually needed in order to achieve the purposes.

4.5.4. Fourth Principle

The Fourth Principle requires data controllers to ensure the accuracy of personal data processed by them, and it requires such information to be kept up to date. Although the requirement to keep information up to date applies only where "necessary", there is no such qualification to the requirement of accuracy. Thus the requirement to ensure that personal data are accurate is an absolute one. There is no definition of "accurate" in the Act, but section 70(2) gives the meaning of "inaccurate":

> *"For the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact."*

An expression of opinion could not breach the Fourth Principle, no matter how unreasonable or ridiculous the opinion.

4.5.5. Fifth Principle

The Fifth Principle 5 refers to data retention. Although there are no specific periods or guidelines in the DPA on how long data should be kept, the Act states that:

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

In other words once an organisation has completed business with a customer and any other legal obligation to keep the data, such as for proving tax submission, has been fulfilled, it should ensure the customer's records are deleted. Failure to do so can also leave an organisation open to compliance issues with Principles 3 and 4.

Data Retention

Organisations should consider the length of time that they will need to keep various types of data. Larger organisations are expected by the ICO to draw up and adhere to a "Data Retention Policy". This is something that the ICO would be expecting to see in the event of a data breach and could be a mitigating factor to receiving a penalty.

Each organisation must consider for how long it will require various types of information and then set specific retention periods, taking into account the needs of the business. These would be determined by other legislation and/or authorities such as Employment Law or Financial Services Authority requirements.

Personal data should always be kept as long as any relevant statutory limitation period. For example, information in an "accident at work report book" should be kept for at least

three years after the date of the accident, as the limitation period for a personal injury claim is three years. In addition, industry sector codes of practice on document retention can be adhered to in most cases.

Some examples of the types of documents and their usual retention period are:

- Job applicants' data (where applicant is unsuccessful)
    - 4 months from the recruitment decision unless the applicant has been notified that their details will be kept on file for consideration of future applications.
- Annual leave information
    - 1 year from the end of the year in which the annual leave was taken.
- Disciplinary records
    - 6 years after conclusion of the disciplinary process.
- Salary details
    - 2 years after the worker has left the employment.
- Accidents on the premises
    - 3 years from the date of the accident

Data Destruction

Data must be disposed of safely and thoroughly:

- once the retention period has lapsed;
- as soon as it is no longer relevant; or
- consent to process data is withdrawn
    - The organisation may need to keep some details in list to avoid future communications

All hard drives must be wiped forensically to ensure there is no personal data remaining on the drive. See Section 4.5.7 for more on safe data destruction.

4.5.6. Sixth Principle

Principle 6 states that the data held should "be processed in accordance with the data subject's rights." This means that each person has a right to expect their data to be respected and handled appropriately and at any point that you hold their details they can legally request a copy of the data to ensure it meets the principles set out above.

Part II of the Act stipulates these rights, the more common of which are discussed below.

- Right of access to personal data (see Section 4.7.2 below on Subject Access Requests).
- Right to prevent processing likely to cause damage or distress.
- Right to prevent processing for the purposes of direct marketing.
- Rights in relation to automated decision making.
- Rights of data subjects in relation to exempt manual data.
- Compensation for failure to comply with certain requirements.
- Rectification, blocking, erasure and destruction.
- Jurisdiction and procedure.

Preventing Processing

An individual may request that a data controller cease processing personal data relating to him/her where damage or distress is likely to be caused by that processing.

Direct Marketing

An individual may request in writing that the data controller cease, or not begin, processing for the purpose of direct marketing, personal data of which he/she is the data subject.

The data controller will need to maintain a record of individuals that have indicated they do not wish to receive direct marketing materials, so that these details are suppressed from future marketing campaigns.

Automated Decisions

A data subject has the right, by notice, to prevent a data controller from taking evaluation decisions concerning him or her by automated means alone. For a decision to be an automated one, there generally must be no human intervention at the point/time of the decision, thus automated decisions are not common. The right relates only to those evaluation decisions that would significantly affect the individual.

Use of information produced by an automated time recording system for promotion-at-work decisions is an example of processing that would fall within the category of automated decisions. Recruitment decisions and credit scoring may also involve automated processing.

A data subject has the right to appeal to a court if a Data Controller is refusing to rectify, block, remove or destroy data relating to their person. If the court rules that the data subject is entitled to action being taken by the Data Controller it can force the latter to respond accordingly. This can also mean rectifying any decision taken by the Data Controller or any third party that the information has been shared with, if the data were inaccurate and as a consequence the decision taken was detrimental to the data subject. This right was challenged at the ECJ in 2014 in a landmark case, where the ECJ ruled that the data subject was entitled to have out-of-date, irrelevant data removed from a search engine's results. More commonly known as the "Right to be Forgotten" case, the Google v Costega Gonzalez ruling is discussed in more detail in Section 4.10.2.

4.5.7. Seventh Principle

The Seventh Principle requires that:

> *"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."*

Organisations must therefore consider appropriate "technical" security arrangements, both internal and external, including password protection, virus protection software, firewalls, data encryption, and building security measures. Laptops must never be taken off-site unless adequate security precautions have been taken, which will usually include encryption of the hard drive.

The organisational measures include the need to train staff in both data protection law and in the organisation's internal data handling policies and procedures. Manual data (paper data in relevant filing systems) should be stored in lockable fireproof cabinets, and a clear desk policy is recommended.

Security should also be borne in mind when personal data are being destroyed. Rarely, if ever, will it be appropriate to dispose of paper-based information without shredding or burning. Relevant IT expertise should be sought before destroying electronic media, and hard drives containing personal data, even if files on the drive have been deleted, should be forensically wiped so the data are not recoverable. A certificate of proof of destruction should be sought and kept on record for each disk disposed of.

Where personal data are to be made available outside the organisation, security is an important consideration. Rarely, if ever, will the sending of unencrypted data held on a CD or memory stick by post by acceptable.

The DPA does not require any specific security measures per se. Most organisations will choose to encrypt the hard drives of laptops that are taken off-site in accordance with the ICO's very strong guidance on the point. Some organisations will also choose to comply with ISO27001:2013 *"Information technology — Security techniques — Information security management systems — Requirements"*, (an internationally recognised standard in information security), although there is no legal obligation to do so.

Using Third Parties to Process Data

Where processing of personal data is carried out by a data processor on behalf of an organisation (outsourcing of one or more functions), the organisation must:

a) "choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
b) take reasonable steps to ensure compliance with those measures."

Data controllers remain responsible under the DPA for the processing carried out by their data processors. Data processors have no DPA obligations themselves, since the provisions of the DPA apply only to data controllers.

Examples of when an organisation might use a data processor include: the use of a call centre; database management; mailing houses; payroll; and web hosting.

Checklist for organisations using "data processors"

1. Ensure that the processing by the data processor is undertaken only in accordance with the controller's instructions (DPA requirement);
2. Ensure that all relevant staff members at the data processor are adequately training in data security measures and procedures (highly advisable);
3. Ensure that there is a contractual obligation on the data processor to implement specific security measures, both in terms of physical security and technological security, such as protection from corruption of data by viruses, and consulting the organisation before changing any such measures (DPA requirement);
4. Ensure the data controller has rights of access to and inspection of the processor's premises and systems, to check that relevant security measures are being appropriately implemented (useful and advisable in many cases); and

5. Restrict the data processor's ability to sub-contract any of its obligations or impose appropriate mechanisms to ensure compliance by the sub-processor (highly advisable).

4.5.8. Eighth Principle

The Eighth Principle refers specifically to the transfer, including storage, of the data to another country outside of the EU border.

> "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."

When transferring, or making available, personal information abroad, organisations should take into account to the limitations on foreign transfers. Foreign transfers can occur in a variety of different ways, for example:

- an organisation renting customer data to a non-EEA country for marketing purposes.
- an organisation is bought out by a non-EEA organisation and transfers its company database to that country.
- an email containing customer details is sent from a company in the UK to someone in a non-EEA country.
- a digital file of oral dictation is sent to a non-EEA country for typing up as written documents.
- an HR Department of a multi-national company is relocated from the UK to a non-EEA country.

In each case organisations should review systematic data transfers to ensure that either:

- information is not transferred or made available outside the protected zone (the European Economic Area ("EEA") plus the "safe countries" (see Appendix 1); or
- that an appropriate method to legitimise the transfer is in place (e.g. model contracts or binding corporate rules - described below); or
- that an appropriate Schedule 4 DPA reason applies, which provides for a legitimate need for the data to be transferred either at the behest of the individual,

the organisation or the authorities. These are very similar to those in Schedule 2 and 3 (for sensitive data) but specifically for information that does not fall under another one of the processing conditions of Principle 8.

Model Contracts and Binding Corporate Rules

The Commissioners have approved the following kinds of transfers:

- **Model Contracts** – There are four approved sets of model contractual terms for transfer of personal data to non-safe countries, although only 3 are available to new agreements as one has been decommissioned. Model contractual clauses have been approved to be used in their entirety, unchanged as they provide for both parties (data exporter and data importer) to be jointly and severally liable to the data subjects in the event of any breach occurring. Any changes made to these models should be reviewed by legal experts to ensure the changes still provide adequate protection for the data subjects. Any of the models can be selected and they are specifically designed to suit Controller to Controller or Controller to Processor situations. The model contractual clauses can be downloaded from the Model Contract Clauses page on the ICO website (2012).
- **Binding Corporate Rules** – BCRs are specifically aimed at facilitating the transfer of data between subsidiaries and parent companies of a global or international organisation and allow for intra company transfers only. Organisations are recommended to use the form provided by the Commission, known as "Article 29 Working Group, Working Paper 133", which can be accessed via the Europa website (2016) along with information and guidance on the process to follow. The rules must be approved by a relevant data protection authority in one of the member states, selected as the lead authority by the organisation, and show that they provide adequate protection for data transferred. Once approved it is the responsibility of the lead authority to circulate the proposed BCRs to all other member state authorities to seek their approval and coordinate the responses.
- **EU-US Privacy Shield** (formerly Safe Harbor Agreement see previous Section 3.2.5.4 for more on how this agreement came about and the key requirements). This is discussed in more detail in Section 4.5.8.1 below.

4.5.8.1. Transferring data to the US

Where an organisation has significant dealings with a US company or parent, it is necessary to provide guarantees that the data will be protected as it would if the organisation was operating solely within the EU. However, the US is not deemed by the

EU a safe country for data protection; despite there being a number of laws in place in the US to safeguard personal data (discussing these is outside the scope of this research) they tend to relate to specific industries or business models and as so, are seen to be too complex and onerous for individuals in the EU to navigate if they need redress due to a data breach. The system in place in the US is also chargeable for anyone wishing to seek redress, which is a significant barrier for many individuals. This complexity, cost and lack of transparency are amongst the reasons that it was felt necessary to come to an agreement between the US government and the EU to offer EU citizens protection more akin to that offered by EU organisations, particularly given the level of penetration of US organisations operating in the EU.

In 2001 a set of principles were agreed upon and companies wishing to operating within the EU or process data of EU citizens (other than those within the telecommunications and financial services sector) were requested to self-certify via the "Safe Harbor" scheme and effectively promise to adhere to the privacy rules it stated on trans-Atlantic data imports/exports. However, an EU citizen, Max Schrems, challenged the agreement and in October 2015 the ECJ ruled that Safe Harbor in fact did not in practice pass the adequacy test for transfer of data. Details of the Schrems case are provided in Section 4.10.4.

EU-US Privacy Shield

This was a key ruling by the ECJ and had significant consequences for the many companies relying on the Safe Harbor agreement to operate legally in the EU, some of them being some of the largest technology organisations globally such as Facebook, eBay, Amazon, Google, etc. However, the Court ruling had actually been seen an inevitability by many who had already questioned the effectiveness of Safe Harbor against the unauthorised access to the data of EU citizens by US authorities. The process of renegotiating the terms of the agreement were already in place and a number of documents had already been produced by the Commission committees debating what the key points of any new agreement should be.

An emergency meeting of the Article 31 Committee (the group of representatives of the data protection authorities in the member states) was convened to start the process of creating a new agreement immediately. In the meantime a moratorium was placed on all complaints specifically relating to the transfer of data for several months to allow time for the Committee to find a solution, although the Hamburg data protection authority did

actually break this and in June 2016 fined three organisations for still using the Safe Harbor agreement to transfer data. After months of negotiation the new EU-US Privacy Shield was brought into force by the publishing of the Commission's Decision C(2016) 4176 on 12th July 2016 that amended its draft Decision published on 29th February 2016. A new Privacy Shield Framework website (2016) was created to provide more information to organisations required to sign up to this new self-certification system. This new agreement also includes the EEA countries, Iceland, Norway and Lichtenstein.

The new system is very similar to the old one in that it is a self-certification scheme with the same principles to adhere to as the Safe Harbor scheme. The key differences are those relating to oversight, indiscriminate surveillance and redress. It will now be the responsibility of the US Department of Commerce to ensure that companies signed up to the scheme are meeting the conditions stipulated. The government have obtained some concessions over bulk data collection from the intelligence agencies, who have agreed to only limit their activities to only persons of interest. Any complaint from an EU citizen should be handled by the correct authority swiftly. There are several ways to make a complaint depending on the resolution method the company has selected and, unlike with the Safe Harbor agreement, the procedure is now free. The EU has issued a guide for citizens to use in the event they should wish to make a complaint.

Critics of this new agreement say that rather than delivering legislative reform from the US all it offers is some political reassurance that the US authorities will act with restraint when it comes to bulk collection of EU citizens' data. An undertaking from the intelligence agencies stated that only those citizens deemed a target would have their information collected and the rest of the data would be filtered out. How this is to be carried out and whether it is carried out under a regime of secrecy with the intelligence services remains questionable. However, the role and independence of the Ombudsman has been increased in this final agreement to accept complaints from individuals concerned about surveillance and allow the Ombudsman to carry out a thorough investigation.

Another issue raised by the Privacy Shield agreement is that of 3rd party sub-contractors who are expected to adhere to the standards of the agreement without having to be signatories of it. It remains to be seen whether the agreement provides adequate recourse for an EU citizen complaining of a data breach caused by the 3rd party; will the primary organisation first have to claim breach of contract of the 3rd party by taking them

to court first and, if so, how likely is this to happen. It will also need to ensure that the 3rd party can provide the same restricted access to its data from the intelligence agency and authorities as the Privacy Shield company, something that will be very difficult to do. Many contracts currently in existence will need to be renegotiated, particularly those involving another organisation outside of the US and EEA.

Data retention rules have also been changed to ensure that all data is deleted once it is no longer relevant or deleted/returned if someone is removed from the agreement list. In attempting to remedy one issue this however creates another as it does not state how a company removed from the list will be made to comply with this requirement if it is no longer bound by the agreement.

Once the Regulation comes into force the onus will be on EU companies to comply with the new legislation but if a company is transferring data to the US or using systems provided by a US organisation it may find it difficult to comply with some issues. These may include responding to Subject Access Requests in the required time, or adhering to a "Privacy by Design and by Default" approach to IT systems.

It is widely expected that this new agreement will be challenged in the same way as the Safe Harbor agreement so it is anticipated that alternative methods to a self-certification system of safeguarding data will need to be sought moving forward and the preferred method for many in the Commission and data protection authorities would be to up improve data protection legislation in the US.

4.6. Notification

Unless an organisation is deemed exempt, all organisations that process personal data, and are therefore effectively Data Controllers must be listed on the publicly available register, maintained by the ICO. The process of registering is known as "notification".

The current annual registration fee is £35 for most organisations and £500 for larger organisations (250 or more staff and a turnover in excess of £15.0 million – for public authorities the test is just whether they have 250 staff or more).

When registering an organisation must state:

a) information about the organisation concerned (such as name and address);

b) the purposes for which personal data are processed by the organisation;
c) the categories of data subjects and types of personal data used by the organisation;
d) the types of person/organisation to whom the information may be disclosed; and,
e) whether any personal data are set outside the European Economic Area.

Organisations are able to draft their own registration entry; the ICO's website maintains a list of "template" descriptions of processing activities, which cover most types of organisations. However, if they are not sure how to complete the registration form correctly they can fill in a form on the ICO's website and email it to the ICO who will then prepare a draft registration entry for the organisation to check before payment is made and the registration confirmed. In either case care should be taken that the template matches the actual processing undertaken by the data controller.

It is a criminal offence to:

- process personal data without an appropriate entry on the register of data controllers unless an exemption exists;
- to fail to notify the ICO of any changes to a data controller's processing activities within 28 days when such changes affect the accuracy of the register entry; and
- process personal data in a manner which is incompatible with the data controller's register entry.

The exemptions (which are rarely applicable) include processing activities which are carried out only for the purposes of:

- staff administration
- accounts and records
- advertising, marketing and public relations.

In the case of exemptions, organisations' Data Protection Officers (or equivalent) should:

- check that all relevant data processing is either exempt from the requirement to notify or that a relevant entry has been made on the notifications register;
- ensure that the entry accurately reflects the types of data processing undertaken by the organisation; and
- oversee the process of keeping the register entry up to date.

An organisation's data protection notification must cover all instances of personal data processing in the organisation, not merely those that occur in the HR or marketing departments. Thus organisations should ensure they have captured all relevant purposes of data processing.

4.6.1. Processing of Data in Multiple Member States

If an organisation wishes to conduct business in a number of EU countries it only needs to be register its activity in one country, usually the one where it is most established. There is no requirement under the Data Protection Directive to notify the authorities in each country. However, as has been discussed previously in this report, due to the fact that the Directive allows each member state to determine the national legislation, each country that a company processes data in could have different regulatory requirements. This does not mean that a company can take advantage of a national regime that has less strict processing compliance rules as the EU Commission are very clear that any attempt at "forum shopping" of laws will not be tolerated. It is therefore very important that the local data protection laws in each member state are fully understood and adhered to as to what is permitted in one country may not be in another. What needs to be notified to the DPA may vary considerably. This is covered in Article 4 of the Data Protection Directive.

In 2010 the Article 29 Working Party felt it necessary to further clarify the scope of the application of the Directive on national legislation by issuing an Opinion. The paper acknowledges the complexity of organisations processing in a different country to the one they a Data Controller in. It states that the "applicable law and the jurisdiction in relation to any given processing may not always be the same" and that "Article 28(6) implies that the national data protection authorities should be able to exercise their powers when the data protection law of another Member State applies to the processing of personal data carried out within their jurisdiction." Article 4 is in force if an organisation has an "establishment" in a member state however the Directive does not actually define what is meant by an establishment although in its preamble it is defined as "an establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements" irrespective of the legal persona of the organisation in the member state. There are several considerations to take into account when processing in different member states and the required action would depend on the specific combination of the following factors: the degree of involvement in the establishment and the nature and origin of the activities.

The paper sets out a number of scenarios and what national law should be adhered to in each:

1. Data Controller is in member state a)
   processing activity takes place in member state a)
   on citizens in member state a)
   then applicable law is that of member state a).
   An example of this kind of situation would be a GPs clinic.
2. Data Controller is in member state a)
   processing activity takes place in member state a)
   on citizens in member state a and b)
   then applicable law is that of member state a).
   An example of this kind of situation would be an ecommerce website.
3. Data Controller is in member state a)
   processing activity takes place in member state b) by a Data Processor
   on citizens in member state a)
   then applicable law is that of member state a) with regard for Data Processor to adhere to member state b) laws and may require coordination between DPAs in each country.
   An example of this kind of situation would be an organisation using invoice factoring services in another member state.
4. Data Controller is in member state a)
   processing activity takes place in member state b)
   on citizens in member state b)
   then applicable law is that of member state b).
   An example of this kind of situation would be an organisation with a satellite office in another member state whose activities are aimed at people in that member state.

A fifth situation was highlighted in a legal case relating to processing across member states was brought before the ECJ in 2015. In essence it related to a Data Controller in one member state who had a website in another member state aimed at citizens of the second member state. Despite the main establishment of the organisation being in the state of the Data Controller there were deemed to be sufficient exercise of activity and stable arrangements in place in the second member state for the ECJ to rule that the

laws of that state applied. However it also ruled that the sanctions for a data breach would need to be imposed by the authority in the member state of the Data Controller. This case is discussed further in Section 4.10.3.

4.7. Compliance

It is common for most medium and large organisations to employ at least one person who is ultimately responsible for compliance with the DPA within the organisation. This person is often known as the Data Protection Officer (DPO) but may also have the job title of Information Governance Officer, Information Compliance Manager, or a similar title.

A DPO should have a very good understanding of what the business does and how, as he needs to have full knowledge of the types of personal data held by the organisation, where it is located at the different points during the business' processes, who has access to it and how it is processed. Some of the undertakings a DPO is responsible for include:

- ensuring that the notifications register entry to the ICO is kept up to date;
- ensuring the organisations compliance with the 8 data protection principles;
- ensuring that relevant staff are trained in their responsibilities under the DPA;
- ensuring that staff are aware of the consequences of their breaching data protection requirements, including any disciplinary procedures that result from a breach;
- providing expertise during any major strategic business decision so that changes can be implemented with appropriate attention to data protection;
- offering advice and guidance to information systems team regarding data protection compliance;
- handling requests for personal data under the "subject access" provisions of the DPA; and
- keeping knowledge of the current legislation and compliance up-to-date.

This section details some of the key documents and processes that organisations are required to provide to show and prove compliance.

4.7.1. The Fair Processing Notice

When personal data are collected by an organisation, the organisation must give, or make "readily available", to relevant data subjects a statement of the following:

- the identity of the data controller;
- the purpose or purposes for which the data are intended to be processed; and
- any other information which is necessary to enable the particular processing to be fair

The requirement to provide "fair processing" information (sometimes referred to as a "fair processing", "fair collection" or "privacy" notice or statement) exists whether or not the personal data are obtained directly from the relevant individual. However, in the case where the data are obtained indirectly, the statement does not have to be provided if to do so would constitute disproportionate effort.

Organisations should ensure that all documentation on which they collect personal data meets the fair processing information requirements in the DPA. For example:

- the employment application form
- new starter details form
- customer details form
- membership details form
- supplier details form
- the organisation's website – privacy policy

The European Commission favours a multi-layered approach to privacy statements, whereby (in appropriate cases) a small amount of information is made available at the point of data collection, and is supplemented by a larger quantity being readily available elsewhere.

4.7.2. Subject Access Requests

Where personal data are being processed by, or on behalf of, an organisation, any relevant individual (e.g. member of staff, customer) is generally entitled by making a subject access request to be informed how the data are being processed and to be given a copy of all the personal data held on him/her in a permanent form.

Failure to comply with this right is the most common reason for complaints to the ICO. It is therefore important for all relevant staff members to be able to detect a subject access request being made and to handle it appropriately, which will usually mean passing it on immediately to the Data Protection Officer (or equivalent).

In addition to being able to obtain a copy of information, an individual is entitled to be given:

- a description of the personal data being processed;
- a description of the purposes for which the data are being processed;
- a description of the likely recipients of the data (to whom the information might be disclosed by the data controller);
- information that the data controller has on the source of the data (where all or part of the data originated from); and
- the logic behind any decisions that were automated.

This is a powerful right and one which can involve data controllers in considerable administrative time and expense. It is necessary to search all of the organisation's relevant systems (electronic and paper) for personal data relating to the requestor.

Before responding to access requests, data controllers should take reasonable steps to verify the identity of the person making the request.

Data controllers can charge a fee for handling an access request where they wish to do so. The maximum fee that may be charged depends of the type of request being made:

- Credit report (£2)
- Education records (£50)
- Health records (£50)
- All other records (£10)

Data controllers have 40 days from the receipt of the request in which to comply. The time period starts to run from the date of the receipt of the request or the date of receipt of the payment (and/or identification documentation), whichever is the later.

The right of subject access is extremely wide-ranging. Unless a relevant exemption applies, an individual is generally entitled to see their personal data contained in all locations, including but not limited to:

- appraisal records;
- disciplinary records
- meeting minutes
- sickness records
- performance review notes
- emails stored on any system in the workplace
- interview notes
- marketing information
- client files
- references received from 3rd parties

The right of subject access is a right to see personal data, not to see documents per se. It should be noted that an individual is entitled to see only his/her own personal data but is not generally entitled to receive any information which relates to anyone else. Sometimes however information relating to someone else will constitute the personal data of the requestor.

Exemptions

Over twenty exemptions from the right of subject access are available to data controllers but the scope of these is complex and where an exemption is to be considered the nature of the situation should be considered carefully. None are generally and universally applicable to any particular type of organisation or sector – thus the access right applies against all data controllers.

The most commonly used exemptions are:

- *confidential references* – the author/giver of a confidential reference is exempt from the need to disclose that reference.
- prevention/detection of a *crime* (e.g. certain CCTV images)
- material disclosing *third party information* – an organisation can choose to withhold third party information from the data subject making the request in certain circumstances but should disclose it where the relevant third party has given consent

or where it is reasonable to do so. It should be noted that there is no obligation to ask for consent from the third party. Compliance is often achieved by redacting copy documents prior to disclosure (blacking out text in document or recreating information in a new document minus the third party information).

- personal data consisting of information protected by *legal professional privilege*. This captures certain information processed for the purposes of obtaining legal advice or for use in legal proceedings (e.g., communications with the organisation's lawyers regarding the dismissal of any employee).
- *management forecasting* – personal data used for this purpose is exempt from disclosure for as long as the management forecasting activity continues.
- *negotiations* – personal data used for this purpose is exempt from disclosure for as long as the negotiations continue.

In addition, there is a limited exemption to the requirement to provide a permanent copy of the information:

- disproportionate effort – rarely, it may be possible for a data controller to show that the effort that it would take to retrieve the requested information (so that a permanent copy can be supplied) is too great. However, the data controller must still furnish the requester with information as to description, source, recipients and logic and should seek to arrange an alternative way for the individual to view the data (such as attending the data controller's offices).

4.8. Enforcement

Data protection law is enforced in the UK by the Information Commissioner's Office (ICO) and the ICO has the powers to implement a number of measures against organisations that are in breach of one or more Principles of the Act. These range from advice on how to better comply with the law to quite severe monetary penalties for more serious breaches or serial offenders. The current approach to enforcement is one of education rather than punishment. The ICO prefers to work with organisations to improve their compliance rather than have to deal with the aftermath of a data breach.

The ICO has stated that all staff members that use personal data in their jobs (which is likely to be the vast majority of people in most organisations) must be given basic data

protection training at the induction stage with updates, reminders and further training being provided as appropriate. Senior staff should receive more in-depth training. Staff members who did not receive training at their induction should be scheduled for training as soon as reasonably feasible. Almost all of the high profile data breaches that attract media attention could have been prevented by appropriate training of staff members and the introduction and implementation of suitable procedures for managing data.

Ideally data protection policies should be in place regarding use of staff data and customer data that clearly outline the steps that employees should take to ensure the maximum protection is afforded to personal data in all circumstances. Organisations should also produce policies detailing the expectations of the organisation as to how employees should use technology and communications facilities provided and guidelines on email usage, in particular the sharing of any personal data by this medium.

Offences

Breaching any one of the principles constitutes an offence but how it is dealt with will dependent on the circumstances leading to the breach and the impact it is likely to have on the data subject(s). The main offences that the ICO deal with are:

- failure to notify ICO of processing or to make changes to a notification;
- obtaining or disclosing personal data without the required consent either from the data subject or the data controller;
- failure of a data controller to take adequate security measures against data being lost, stolen, destroyed or disclosed; and
- failure to act on a formal notification from the ICO.

Complaints to the Commissioner

If an individual feels that he/she has been negatively affected by the processing of personal data, a request can be made to the Information Commissioner carry out an assessment to determine if the processing complies with the DPA. The Commissioner must carry out the assessment but can decide on the method the assessment will use depending on the circumstances of the request, for example:

- whether the processing is considered to be having a significant impact on the data subject;
- whether there has been a considerable lapse of time since the processing took place; and
- whether the person requesting the assessment is the data subject or entitled to make the request on their behalf.

There are a number of legal instruments at the disposal of the ICO. A full list of all the legislative means available to the ICO can be found in Appendix B of the Data Protection Regulatory Action Policy guide on the ICO website (2013). As the ICO states on its website, these tools are not always used in isolation and it is common to see a variety being used in conjunction or if an issue has escalated due to the organisation not complying with earlier measures imposed. The more common ones are discussed here.

- *Audit*

  The ICO has the power to conduct on the spot audits in any public sector organisation without giving prior notice. However, it is only allowed to audit private sector companies with the consent and prior knowledge of the organisation or if this is not given and/or there is a reason to suspect criminal behaviour a search warrant can be applied for from a judge that can give the ICO powers of entry, search and seizure.

- *Information Notice*

  If the ICO requires any information to help it determine whether an organisation is complying with the Act, or to investigate how a breach occurred, it can issue an Information Notice to the organisation, who by law must comply. Failure to do so can lead to further sanctions.

- *Non-criminal enforcement*

  Often for a first time offence that is not seen as being high risk to data subjects the ICO can issue an undertaking to the organisation to take certain measures to improve its compliance. This is the most often used type of penalty. Not acting on an enforcement undertaking can lead to further sanctions being imposed on the organisation. The ICO can force "Stop Now" orders on an organisation to require it to cease processing activities or take specific steps to amend a process if there has been a breach or to stop a breach from occurring. These are called Enforcement Notices. An Undertaking can be issued to ensure that an organisation commits to taking a particular course of action in order to improve its data protection compliance.

- *Civil monetary penalties*

  The ICO currently has the power to fine organisations up to £500,000 per data protection breach, depending on the level of severity, as it sees fit. It is usual that a

Notice of Intent will be issued prior to a fine to prepare the organisation for the monetary penalty to follow and to provide them with an opportunity to appeal the decision. The ICO has the right to issue fines up to and including the maximum but needs to refer to a court if it feels that its powers are insufficient to apply the correct penalty.

- *Criminal prosecution*
  Anyone found guilty of deliberately breaching the Data Protection Act, for example a Section 55 offence, a court may impose a prison sentence of up to 2-years on the perpetrator.

- *Compensation for Damage/Distress*
  A data subject that believes a breach of the Act has caused him/her damage or distress is entitled to request compensation. However, such claims have so far been difficult to prove and are therefore quite rare.

4.9. Secondary and Related Legislation

There are quite a number of secondary and related laws that may overlap or work in conjunction with data protection legislation. It is outside of the scope of this report to discuss any of them in great detail or to list them all. However, several of these laws are briefly covered below.

4.9.1. FOI 2000

The Freedom of Information Act 2000 is a piece of legislation that allows any member of the public to access non-sensitive information from any public sector organisation such as all government departments, local authorities, the NHS, state schools and police forces. It does not as yet cover charities that receive grants or certain private sector organisations that perform public activities. However there is considerable pressure on government to widen the legislation to include these. If the information has not been made publically available the individual has the right to make a request for a copy of the information. The types of information that can be accessed is quite far-reaching and as well as the obvious printed documents, meeting minutes, computer files and letters, it is also possible to obtain copies of emails, photographs audio and video recordings. It also covers any handwritten notes, transcripts or original audio recordings of telephone

conversations, CCTV footage, data sets and meta-data. There is usually a 20-day limit on the time to complete the request.

4.9.2. PECR 2011

As previously discussed in Section 3.2.5.5 organisations must also comply with the Privacy and Electronic Communications Regulations 2003 and 2011 in regards to electronic communications including telephone, fax and email marketing and use of cookies.

4.9.3. Surveillance and National Security Legislation

Exemptions exist in data protection legislation to allow disclosure and processing of an individual data if that person is under investigation by police and criminal authorities however any requests for information should be accompanied by the relevant authorisation. Conversely data protection legislation, particularly in light of the need to amend the Safe Harbor agreement, does not allow indiscriminate bulk collection of data. It has been revealed by the NSA whistle-blower, Edward Snowden, that the UK intelligence services have been conducting covert mass data collection of UK citizens since at least 2007. The implications of this revelation on data protection legislation are very significant and it is anticipated that there will be a challenge to this activity forthcoming. In an attempt to legitimise the untargeted data collection there have been several attempts by the UK parliament to introduce laws to allow it to continue before it is made to cease by a court. One of these pieces of legislation was the Regulation of Investigatory Powers Act 2000 (RIPA), which was passed into law, although after a challenge, the ECJ ruled that parts of the Act did in fact allow for violation of the Data Protection Directive and demanded that the UK Government repeal parts of the Act pending proposing new legislation.

The Data Retention and Investigatory Powers Act 2014 (DRIPA) is a piece of emergency legislation that was introduced to amend RIPA and as a response to the defeated Data Retention Directive. It is due to expire at the end of 2016 and new legislation is required to succeed it.

The latest piece of legislation to enter into the legal arena is the Investigatory Powers Bill 2016 currently at the Committee Stage in Parliament. Whilst it is outside the scope of this report to discuss this legislation in any detail it is important to note that the proposal for all telecommunications providers to capture all web traffic for all users and store this

data for one year is proving extremely controversial and many data protection advocates and activists around the globe believe this to be a draconian law. It will place a considerable amount of extremely private and personal information in the hands of private companies and the government and it is widely seen as the greatest assault on data protection legislation to date. Nevertheless, the UK Home Office believe that the Bill is compatible with the EU Convention on Human Rights. It remains to be seen whether this will be challenged in an EU court if the Bill is passed into law and just what the ruling will be.

4.9.4. Digital Economy Bill

The Digital Economy Bill was presented to Parliament in July 2016. As well as aiming to provide an infrastructure to allow the UK to develop first class digital services for the future, one of its remits is to provide greater flexibility for how public sector organisations use and share data.

Part 5 of the Bill specifically focuses on Digital Government. This will include personal data, which with the adoption of this Bill will become more centralised as the government aims to move more services online. According to the news brief published on the Government's website the types of services the Digital Economy Bill aims to digitise are as follows:

- *"allowing public authorities to share personal data with other public authorities in specific contexts in order to improve the welfare of individuals, for example the Troubled Families programme*
- *improving access to civil registration data like births, deaths and marriages, so that public authorities do not send letters to people who have deceased and to make processes easier for users*
- *helping to detect and prevent the losses government currently experiences due to fraudulent activity each year*
- *providing new mechanisms to detect and collect public sector debt, that currently stands at over £24 billion in monies owed to government*
- *helping individuals to manage their debt by providing a means of support*
- *making it easier to use data for research purposes so that official statistics are more timely and accurate"*

The Digital Economy Bill will create some additional security risks for protecting citizens' data, particularly as many of the services it identifies as being targeted for centralising

would be classed as sensitive data. However, if all local authorities put effective measures in place to protect personal data this would go a long way to ensuring that some of these risks are minimised before the programme of digitisation accelerates.

It will be necessary to look into this area in more detail to determine if there will be further issues to take into account but this is outside the scope of this report.

4.10. Cases

Some rulings of the ECJ have had far-reaching consequences for the processing of data outside of the EEA. Several of these key cases are outlined below.

4.10.1. ECJ: C-101/01 (judgment of 6 November 2003) / Lindqvist

The Lindqvist case helped to define the scope of what was classed as processing of personal data and the definition of transferring of data to third countries. Bodil Lindqvist, a Swedish national had posted information on her personal website including names, addresses and contact details of individuals she had worked with during a period of volunteering at a local church. She was taken to court locally by one of the individuals for breach of Directive 95/46/EC. The national court ruled against Lindqvist deciding she had indeed violated the right to privacy of the individuals by not obtaining their consent before publishing despite the fact that this had been done in the context of her not-for-profit activities and her argument that she had been exercising her freedom of expression by posting. It also ruled that by posting the information on her website she had actually transferred the data to a country outside of the EEA.

Lindqvist appealed the decision of the court in Sweden and the case was referred to the ECJ. The ECJ upheld the decision of the Swedish court that Lindqvist had in fact processed personal data without the individuals' consent by posting it on her website despite her claim that this was in the course of her non-profit making activities, which significantly broadened the scope of what was deemed as personal data within the jurisdiction of the Directive. Its ruling failed to address her other claim that she was exerting her right to freedom of expression. This ruling raised important points regarding the processing of information by individuals in certain circumstances, not just companies; and via the Internet, therefore having regard to the medium of publishing the data.

Another interesting outcome to the ECJ decision was support for Lindqvist's claim that she had not transferred data to a third country. The ECJ ruled that this was not the case as Lindqvist had not deliberately sent the information to someone in a third country by posting it on her website. A caveat to this decision was that the server infrastructure was not located in a non-EEA country. The rise of the use of cloud services has brought this into question much more recently, especially as many web hosting companies do not openly disclose the whereabouts of servers for security purposes.

4.10.2. ECJ: C-131/12 (judgment of 13 May 2014) / Google v Costeja Gonzalez

More commonly known as the "Right to be forgotten", the ruling on this case had particular consequences for search engines. After a newspaper in Spain, at the behest of the national authorities, had published an announcement relating to the forced sale of a house the individual mentioned in the announcement, Mr Costeja Gonzalez, contacted the paper 11 years later to have the announcement removed. He complained that despite the matter of the related sale being resolved many years before, a link to the article was still appearing when his name was entered into a search engine. The newspaper refused to remove the announcement from its website archives citing the official nature of the initial request to publish the article. Mr Costeja Gonzalez then contacted Google Spain to ask them to remove the links from the search results. Google Spain stated it was not responsible for the search engine results and subsequently referred the request to its parent company, Google Inc., situated in California, US, who refused the request citing that the Directive did not apply to it.

Mr Costeja Gonzalez then lodged a request for the newspaper to remove the article and for Google to remove the link with the Spanish data protection authority. The authority rejected the removal request for the newspaper but concluded that Google should remove the link from its search engines. In response to the decision Google Spain and Google Inc., both made separate appeals to the Spanish High Court. Google Inc stated it was not under the jurisdiction of the Directive therefore had no obligation to comply. Google Spain said it had no control over the search engine results. Both companies argued there was no processing of personal data and that neither could as such be classed as a Data Controller. There was also an added defence that the article had been lawfully published therefore there was no right to erasure.

The High Court merged the two actions and referred the case to the CJEU to respond to questions of interpretation regarding: the scope of the Directive territorially; whether data processed by a search engine could be classed as personal and therefore the companies

providing the search engines deemed Data Controllers; and if the Directive provides for the right for a past action to be erased if it has a negative impact on someone's privacy.

The Advocate General in his Opinion stated that whilst personal data was actually being processed by Google it could not be seen as a Data Controller due to the random nature of the processing and that it was processed using the same methods as non-personal data. However, the Court ruled differently, citing the Lindqvist case, that Google was in fact a Data Controller as the data was processed by automatic means and it did have some control over that process. The Court also ruled that as Google Spain was selling advertising space on behalf of Google Inc., the latter was indeed within the scope of the Directive and therefore obliged to remove the article from its search engine.

It also found that the Directive gave grounds for the right for data to be erased, despite the Advocate General's concerns that future interpretations of this ruling could lead to restrictions of freedom of speech or censorship of the Internet. The ruling made it clear that a distinction should be made between a private and a public person to avoid the decision being used to influence public opinion for example. It was argued that there was the potential for there to be a great economic impact on the search engine organisations however it was deemed that a data subject's rights should be put above this. On the day after the ruling Google subsidiaries throughout the EU received 12,000 requests to remove links.

4.10.3. ECJ: C-230/14 (judgment of 1 October 2015) / Weltimmo

The Weltimmo case was a ground breaking ruling regarding the jurisdiction of one member state's data protection authority to impose fines on a company headquartered in another member state. It went a great deal to framing the discussion relating to a "one-stop-shop" solution of dealing with data protection authorities, as provided for in the new Regulation.

Weltimmo, a Slovakian property company was operating a website aimed at Hungarian citizens that provided a "first month free" offer to customers to advertise properties for sale; subsequent months advertising were chargeable. Despite customers asking Weltimmo to remove ads before the first month had ended the company did not comply with the requests and left them on the site then started to charge for the service. When customers didn't pay the charges Weltimmo passed their details to a Hungarian debt collection agency. A number of customers complained to the Hungarian data protection

authority and the Slovakian company was fined. Weltimmo challenged the fine from the Slovakian authority and the case was referred to the ECJ for clarification. The key determination it sought was whether under Articles 4(1)(a) and 28(1) of the Directive it was within the jurisdiction of one member state authority to fine a company headquartered in another member state.

The ECJ found that under Article 4, Weltimmo did in fact have an establishment in Hungary as it had several websites written in Hungarian that dealt solely with Hungarian properties. The Court also factored in that the organisation had an agent based in Hungary, a Hungarian bank account to deposit its debt collection monies into and a Hungarian post box for receiving mail. However the ECJ also found that Article 28 did not allow for sanctions to be imposed on a company residing in another member state and thereby imposing its own laws in that jurisdiction. The Hungarian authorities had to defer the sanctioning powers to the Slovakian authorities.

4.10.4. ECJ: C-362/14 (judgment of 6 October 2015) / Schrems

This was a landmark case that would not only affect the interoperability of the EU member states but the ability for some of the largest global organisations to function legally. It is the first time that the ECJ had to rule in a case of the transfer of data to a country outside of the EEA and was the first challenge to the Safe Harbor Agreement.

In a 2012 paper, Hoboken, Ambak and Eijk, researchers at the University of Amsterdam concluded that the US Patriot Act allowed the US government unregulated access to EU citizens data and violated the Safe Harbor agreement. However, they also concluded that it still required the participation of the organisations holding the data so there was still some restrictions on what they could access, when and how. This all changed in June 2013 when a contractor working at the National Security Agency (NSA) in the US revealed that the NSA and the British intelligence agencies (GCHQ) were conducting a massive surveillance program that consisted of collecting and storing email and web traffic of all US (via the GCHQ) and EU (via the NSA) citizens. The political repercussions of the revelations were felt throughout the EU as realisation dawned that they were being spied upon by a supposed ally. However, despite a number of public statements from the EU Commission on the potential invalidity of the Safe Harbor agreement in light of the new information, no new agreement, or discussion leading to a new agreement were forthcoming. However, when an Austrian national, Max Schrems, took Facebook to court in Ireland in 2015, for violation of his rights to privacy by failing to

safeguard his information from being collected illegally by the NSA, the EU had to act. Schrems asked the Irish data protection authority to demand that Facebook stop sending his data to the US, as it was within their power to do so under certain circumstances. The Irish authority said it was not within its power to investigate his claim as there was no actual proof that the NSA had accessed his data and that as Facebook was a signatory of the Safe Harbor agreement it was not within its powers to overrule the agreement.

Schrems appealed the decision not to investigate at the Irish High Court who requested a decision from the ECJ. One point for clarification regarded whether a national authority is absolutely bound by an EU Commission Decision or whether it had the power to decide if a country was safe to transfer data to, as this was usually decided by the Commission; national authorities usually ruled in individual cases only. A second point requiring a ruling was whether the actions of Facebook (and consequently all US companies signed up to the Safe Harbor agreement) were adequately able to meet the requirements set out in Articles 7 and 8 of the EU Charter of Fundamental Rights.

In his Opinion statement, the Advocate General Yves Bot (2015) stated that "the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the national supervisory authorities' powers under the directive on the processing of personal data. He considers furthermore that the Commission decision is invalid." Whilst not binding on the Court his declaration had great sway. The Court agreed with his Opinion, which effectively provided the national authorities with the powers to question the adequacy test undertaken by the Commission on a country if the protection of such data is questioned by an individual, and that the national authority's ability to investigate such a claim should remain intact.

Furthermore, Bot continued in his opinion to say that "the law and practice of the United States allow the large-scale collection of the personal data of citizens of the EU which is transferred, without those citizens benefiting from effective judicial protection" and without allowing any redress to remedy the situation by an individual. During the hearing Bot asked the EU Commission's attorney if there was any way of ensuring the US authorities didn't get access to his Facebook data, to which the attorney responded that Bot could always close down his Facebook account. This statement, and the fact that the EU Commission was already in talks with the US government about reviewing the Safe

Harbor agreement, seemed to be proof enough that there were no real safeguards in place for data being transferred to the US. The Court subsequently ruled that the entire Safe Harbor agreement was invalid due to the reasons set out in Bot's Opinion.

5. Introduction of the EU General Data Protection Regulations

The explosion in the amount of personal data available online and being transferred indiscriminately between organisations and across country borders meant that the Directive and varied EU member state laws were no longer fit for purpose, particularly with regards to non-EU companies processing EU citizens' data. When coupled with the introduction of the revised EU framework, that came into force with the Lisbon Treaty, the adoption of the EU Charter on Fundamental Rights elevating data protection to a level of primary legislation, and the requirement to adopt data protection legislation across all law enforcement and public sector as well as the internal market, it was clear that a stronger, more consistent update to the Directive was needed to make it fit for purpose. However, whether it is comprehensive enough to be consistent, or strong, is questionable given that the new legislation is in two parts; the Regulation, which replaces the Data Protection Directive 95/46/EC and is aimed at the private and most of the public sector, and a Directive to repeal the Council Framework Decision 2008/977/JHA, for the police and criminal justice sectors. It will likely lead to discrepancies in how this new Directive is implemented and given the current increased appetite for state surveillance there is a real possibility that laws introduced to enact the Directive in some countries, such as the UK, are likely to offer the minimum protection possible to allow some room for more targeted surveillance laws to work alongside it, such as the proposed Investigatory Powers Bill currently under consideration in Parliament.

The Data Protection Directive made provisions for regular reviews of the implementation of national legislation and to allow the member states to submit proposed amendments as seen necessary. Two reports published in 2003 (First report on the implementation of the Data Protection Directive (95/46/EC), and 2007 (European Commission, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, 7.3.2007, COM (2007) 87 final) highlighted considerable differences of implementation between the then 10 member states, either due to incorrect interpretation of the objectives or choices of approaches to the policy. Some countries favoured a strict regime where others preferred to be much more lenient. The problem with such a divergence was the distinct possibility that it would lead to companies shopping around to take advantage of countries with a lighter touch to base their processing facilities in.

It wasn't until the adoption of the Lisbon Treaty in 2009, however, that the Commission accepted it was necessary to start planning for changes to data protection legislation and launched a public consultation. A key document to come out of this exercise was "The Future of Privacy" (2009), a joint report by the Article 29 Working Party and the Working Party for Police and Justice, who recommended that efforts were placed on:

- clarifying the current rules and principles especially around consent and transparency;
- providing guidance on the design and development of new technologies and processes to strengthen privacy and accountability from the outset of development;
- limiting bureaucratic burdens on companies;
- creating one comprehensive legal framework, which also applied to police and judicial cooperation in criminal matters.

This was the first real acknowledgement that the system in place was no longer fit for purpose and was too complex for the new global marketplace for data. A further report in 2010, "A comprehensive approach on personal data protection in the European Union", proposed stronger rights for individuals, more robust enforcement for breaches and greater measures to deal with globalisation and transfers of data across borders.

The first draft of the Regulation was finally published by the European Commission on 25 January 2012, championed by the then Vice President of the EU Commission Viviane Reding, Member of European Parliament from Luxembourg. The proposal iterated that the existing framework was still sound but that it had "not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity." (European Commission COM/2012/011).

Since the publication of the first draft proposal there were a number of events that contributed to the resulting legislation being adopted under the ordinary legislative procedure (See Section 3.2.4.2). These included various committee meetings and negotiations to navigate the way through and vote on the 4000 plus suggested amendments from special interest and citizen watchdog groups, business lobbyists, and individual member state parliamentary representatives. The resulting Regulation was adopted on 27th April 2016 and comes into force on 25th May 2018, allowing organisations a two year period to make the transition to comply with the new legislative framework.

A comprehensive list of the events leading up to the adoption of the new legislative package and links to all documentation of committees, is available on the website of Hunton & Williams, Data Protection legal specialists (2016), however, some of the more important milestones on the four-year journey to its enactment are described below:

- The EU Data Protection Supervisor at the time, Peter Hustinx, issued an Opinion of the EDPS on the Data Protection Reform Package (EDPS 2012) where, whilst he was mostly in favour of the proposal and praised some of the measures to strengthen individuals' rights, he criticised the decision to have a separate Directive for Law and Criminal Justice, believing this weakened the comprehensiveness of the reform agenda.

- Shortly afterwards (23 March 2012) the Article 29 Working Party issued its Opinion on the proposal showing clear support for measures that encourage more organisations to conduct impact assessments and adopt "privacy by design and by default" development approaches. It responded to concerns from national parliaments that the Regulation and Directive proposed did not dilute the data protection legislation adopted by some governments who wanted reassurance that the legislative requirements would raise the bar rather than lower it. It also echoed the concerns of the EDPS that the separation of legislation into two separate instruments may indeed weaken its overall impact.

- In its report on the data protection reforms from its annual conference, in May 2012, the EU Data Protection Commissioners also largely welcomed the reforms but felt there was still more work to do "...to bring the proposed Directive regarding the area of police and justice more in line with the core principles..." and that "...the transfer of data between private parties and law enforcement bodies are, for instance, still missing."

- The LIBE committee held its first stakeholder meeting to discuss the proposals in May 2012. The outcome of the meeting was the First Working Document issued in July 2012, which set out the general position of the Committee on the proposal to commence the first round of co-decision discussions in Parliament.

- During the First Reading stage of the Parliament, Data Protection Rapporteur, Dimitrios Droutsas (October 2012) released Draft Reports to Parliament, and after MEPs debated the proposal, Jan Albrecht (January 2013), also a Data Protection Rapporteur, published a revised proposal to submit to Parliament for vote that included over 350 amendments to the Regulation and Directive.

- During several months of debate from the internal market, industry, employment and legal affairs committees, the LIBE committee received and voted on over 4,000 proposed amendments to the legislation. Dubbed by many as the most lobbied piece of EU law to date, even more than the EU treaties, the difficult task of agreeing which proposals to adopt was finally completed in October 2013 when the LIBE committee produced a revised version of the Regulation to present to Parliament, who voted on and approved it on 12th March 2014.

- One year later in June 2015 after studying the revised document of the Parliament and having some proposed amendments to that document, the Ministers at the EU Justice and Home Affairs Committee agreed to start "trilogue" negotiations with the Presidency acting on behalf of the Council in the talks with the Parliament and the Commission.

- After a further LIBE Committee vote in December 2015 on the Council proposals, agreement was reached on the document to present to Council for its First Reading. The revised proposal was agreed by the Council in April 2016 and subsequently passed to Parliament for the Second Reading who also voted to adopt the legislation. The final act was published in the Official Journal on 4th May 2016, and entered into law 20 days later, effectively repealing the Data Protection Directive and the Council Framework Decision 2008/977/JHA

5.1. Police and Criminal Justice Directive 2016/680

At this point it is relevant to turn some attention to Directive 2016/680 repealing the Framework Decision 2008/977/JHA on police and criminal justice cooperation within the EU. As well as placing obligations on the authorities in the member states regarding the processing of data transferred across the EU borders, it also regulates the processing of

personal data to countries outside of the EU. More controversially it places data protection obligations on the authorities in the member states processing personal data within their own internal borders. As the new legislation was created under Article 16 of the Lisbon Treaty, and it introduced a new measure in the area of Freedom, Justice and Security, the UK and Ireland are able to exercise their right set out in Article 6a of Protocol 21 to opt-out of any EU legislation in the areas of policing and criminal justice based on Article 16.

The special status of the UK means that the Directive will only apply to a limited extent. Any transfer of personal data cross border will be bound by the new legislation. As the new Directive also places new data protection obligations on police and criminal justice activity within the internal border of the member states in relation to those functions, the UK and Ireland are not bound to apply it as this is effectively a new measure. Discussions that took place pre-referendum appeared to suggest that the UK was considering not adopting the Directive, despite Ireland deciding to do so and thus leaving the UK to be the only member state whose police and criminal justice authorities were not bound by the new data protection rules. Post-referendum, this is an area of the pending legislation that has had little attention and it remains to be seen what will be implemented, if anything, to allow the continuation of cross border processing once the UK withdraws from the EU.

5.2. Key Changes in Regulation

This section of the report looks at the key areas of the Regulation and how these differ from the current Directive and the DPA.

Similar in wording to the Directive but not identical, Article 5(1) sets out the "Principles relating to the processing of personal data"

1. *Personal data shall be:*

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

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

(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 ('accuracy');

(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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(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 ('integrity and confidentiality').

Article 4(1) has the definition of "personal data", which largely remains the same as in the Directive, however, expanded to include online identifiers (IP addresses of devices used to access the Internet), location data and genetic information but only if these are used to specifically identify an individual. "Sensitive" data is renamed to "special category" data and the conditions under which it is allowed to process it are outlined in Article 9. Additions to this category are genetic, biometric data and information regarding sexual orientation is explicitly mentioned.

5.2.1. Scope and Jurisdiction

The Directive placed clear responsibility for the transfer of data to a non-EEA country with the Data Controller, an established entity within the EU, and as such any breach of the Data Protection Act rested firmly with the Data Controller. Prior to the Weltimmo ruling (see Section 4.10.3) there was still some confusion over which national legislation a Data Controller had to comply with if it was established in one member state but also

operated in another one. The Directive states in Article 4(1)(c) that if an organisation was not "established" in a member state it was still subject to the national legislation of the member state if it "for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community." Nevertheless, as the Weltimmo case highlighted, the definition of "established" was not explicit. Article 4(1)(c) also applies to those organisations outside of the EU using processing equipment within the EU. However, this still left processing of EU citizens' data on equipment not established in a member state at risk.

Under the new Regulation there will be much less ambiguity for EU Data Controllers; one set of rules to comply with across all member states will make it much easier for a company to operate in any and all member states should they so wish. For non-EU companies the test for compliance is stated in Article 3(2) as:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

This expansion of jurisdiction will most likely result in challenges as the threshold for determining when an organisation is specifically offering goods or services to an EU citizen has not been clearly defined. Having a website accessible in the EU will not in itself constitute required compliance but, for example, providing the website in a language other than that used in the organisations territory or explanations of shipping requirements to the member state might well constitute establishment of operations.

Non-EU organisations will need to appoint a representative who is established in one of the member states to act as a Data Controller on its behalf. This representative will be responsible for compliance and enforcement.

5.2.2. Member States' Supervisory Authorities

The Regulation will see the creation of Supervisory Authorities (SAs) in each member state. It is likely that the existing Data Protection Authorities (DPAs), in the UK the Information Commissioner, will be renamed and given new expanded powers. A "One

Stop Shop" approach to compliance will be introduced in an attempt to simplify the legislative landscape for organisations and citizens. The burden of notification of processing activities has been removed from the Regulation for most organisations; only those deemed to be processing special category data or data that may present a considerable risk in the event of a breach occurring must pre-register its activity with the SA. Organisations that are processing data in more than one EU member state or transferring data outside of the EEA will also be required to register. Registration should be undertaken in the member state where the organisation undertakes the majority of its processing activities. This SA is known as the "Lead Authority".

There was no power for DPAs to audit within the Directive but the ICO was given the power to audit public sector organisations from the UK government; private sector organisations could only be audited with their consent or with a Court order. Under the Regulation the SAs will have the power to audit both public and private sector organisations without prior consent.

SAs will also have all of the other enforcement and notification powers that the previous DPAs had within their own member state but they will not have jurisdiction to enforce the Regulation in another member state. The Lead Authority will be required to work closely with other SAs in order to investigate and penalise cross-border data breaches. In the event a breach occurs the organisation would report this to its Lead Authority who would then coordinate with the SAs in the other countries likely to be affected by the breach on behalf of the organisation. A citizen of any member state can report a suspected breach to the SA in his/her own member state regardless of where the processing may take place and the SA is required to act on behalf of that citizen and work with other SAs to resolve the complaint.

In order to facilitate this cooperation and ensure there is a standardised approach to enforcing the Regulation, a Consistency Mechanism will be put in place to provide guidance to the SAs. This framework is also expected to help SAs to coordinate enforcement across member states to avoid situations where different SAs may penalise a similar offence heavily in one country and lightly in another. There is likely to be considerable discussion and negotiation once this Mechanism is in place to establish some standard enforcement approaches for different offences. Until some standard offence responses have been determined there is also likely to be delays in penalties being imposed on infringing organisations; the penalty will need to fit the breach well from

the outset as any differentiation in enforcement measures for similar breaches in different countries may lead to challenges in Court over the decision.

A new EU-wide Regulator, the European Data Protection Board (EDPB), will be established to oversee these newly created SAs. As defined in Articles 68-76, it will replace the current Article 29 Working Party with enhanced powers to make binding decisions on enforcement and will become a body of the Union and a legal entity in its own right. In essence the SAs will form one group of companies. The EDPB will also act as an arbitrator in the event of any disagreement between Lead and other SAs.

5.2.3. Accountability

The concept of accountability forms a central theme of the new Regulation. This essentially means that data protection becomes part of the shared values and practices of an organisation and that the responsibilities for implementing the legislation are expressly assigned.

Article 24 of the Regulation sets out the responsibility of the Data Controller and 24(1) states, "the controller shall adopt policies and implement appropriate measure to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation."

The Regulation provides that this should include maintaining documentation, implementing security measures, performing data protection impact assessments, designating a data protection officer, consulting with the data protection authority and data protection officer, and establishing transparent communication with data subjects. However, it is evident throughout the Regulation that there is a desire to ensure a reduced burden on businesses, especially where the likelihood and potential impact of a breach is low. An example of this is the removal of the requirement to register as a Data Controller. Nevertheless, regardless of whether the organisation is required to register, where there is processing of personal data there is still a Data Controller. To offset the fact that registration is no longer required in most circumstances, organisations are expected to keep comprehensive documentation of the procedures they put in place to prove compliance before the event. The greater the risk to the data subjects by the processing, the greater the requirement to put stringent measures in place to avoid a breach. Some of the more time-consuming measures therefore will only apply to medium to large organisations, or smaller organisations that process a considerable amount of

personal data. Article 30 details the information that needs to be made available to the SA if required.

A key requirement for all Data Controllers is the production and accessibility of an Information Notice, more commonly known in the UK as a Fair Processing or Privacy Notice. As already stated earlier in this report, these are a requirement under the Data Protection Act. However, under the new Regulation additional information will need to be included. Article 12 sets out the requirement to notify the data subject and Article 13 describes the information that needs to be made available. As well as the details needing to be communicated under the existing Act, there will now be a requirement to disclose the contact details of the Data Protection Officer, the legitimate reasons for wanting to process the data, how long it will be kept for and any details of a transfer to another country, such as where and why. It will also be necessary to provide a brief overview of the data subject's right to complain, to object to processing and guidance on data erasure.

5.2.4. From Data Processors to Data Controllers

Any organisation that undertakes any processing activity on behalf of another, currently known as a Data Processor, will in future be bound by the Regulation. This means that the Data Processor will now become a Data Controller in its own right. The organisation will still be identified as a Data Processor but there are stipulations under Article 28 of the Regulation that they will also be bound by. There will still need to be a Data Processing contract between the two companies, as set out in Article 28(3), and it is likely that this will look very similar to what should already be in force currently. However, once the Regulation comes into force the company under contract will be equally responsible for compliance with the legislation, and will be held directly accountable by the SA in the event of a data breach, which it is seen to have caused or not prevented, that occurs during any processing activity it is under contract to deliver.

It is still highly recommended that due diligence is carried out by the company outsourcing its data processing activity as regardless of who is held responsible in the eyes of the SA, there is always the risk of reputational damage for the primary data controller in the event of a breach and failure to manage the processing activities of subcontractors is very likely to also see blame for a breach apportioned to the Data Controller.

It will be important to have a clear data breach notification policy between the two parties so that any issues are reported in a timely manner to avoid any further penalties. There are a number of issues that this agreement should aim to resolve such as defining what constitutes a breach and what course of action should be taken in the event of a breach occurring. Other issues to be resolved will include determining the time frames for reporting breaches or, in the event of a serious breach, who should report the breach to the SA. How to notify data subjects, when and who should also be a key component of any contract.

It will also be necessary to have a clear cooperative Subject Access Request policy agreed by the two parties as an individual will have the right to directly request a copy of the data processed being processed by either organisation. To ensure that the SAR is responded to fully within the 40 day period and that potential exemptions and redactions are dealt with in a consistent manner it is important that there is direct and timely dialogue between the two organisations in the event of any request.

5.2.5. Data Breaches and Penalties

Under the Directive it was left to national legislation to decide what the penalties of a breach would be. However, the Regulation takes a slightly different approach to breach management and aims to harmonise enforcement through the Consistency Mechanism.

So far, breach notification has been voluntary in the UK, except for central government offices and the NHS who were mandated by the government to report to the ICO. The voluntary reporting of a breach is seen as a mitigating factor in the administration of punishments. However, the Regulation requires any organisation suffering a data breach to report this to the SA no later than 72 hours after it has occurred as set out in Article 33, unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons". Any delay to this must be justifiable. Under Article 34, the Data Controller must also notify all data subjects individually of the breach if it is "likely to result in a risk to the rights and freedoms of natural persons". In other words, if a breach meets the requirement to require a mandatory notification to the SA then it is highly likely it will also be reported to the data subjects in order that they have as much warning as possible to mitigate the risks. There are circumstances where notification to data subjects is not required; if the data compromised was encrypted, if other measures were taken post

breach that renders the data unusable, or if notification would involve "disproportionate effort" wherein a public announcement might be more suited.

Exactly what constitutes a breach with serious impact however is still open for interpretation and may become an issue that will require further clarification.

Penalties

Article 83 stipulates the conditions under which a penalty is likely to be incurred. Article 83(3) outlines the maximum fines for the various breach categories:

"4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

b) the obligations of the certification body pursuant to Articles 42 and 43;

c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

b) the data subjects' rights pursuant to Articles 12 to 22;

c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

d) any obligations pursuant to Member State law adopted under Chapter IX;

e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to

administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."

Under Article 83(f)(a), the maximum fine for not reporting a breach to the SA can be up to €10 million or 2% of turnover, whichever is the greater. The issuing of high fines is still quite rare and the current climate in the UK is one of carrot rather than stick. Consequently this is a key step change in the approach to be taken to breaches by the new Regulation and requires a similar step change in the attitude to data protection in organisations.

Article 84 gives powers to each member state to determine the rules regarding penalties other than those set out in Article 83, subject to administrative fines. Each member state should ensure that the penalties it sets are "effective, proportionate and dissuasive" and governments should communicate the list of infringement measures it will take to the Commission by 25th May 2018.

6.1.1. Dedicated Data Protection Officer

Section 4, Articles 37 to 39 sets out the requirement for some organisations to employ, or contract out, a Data Protection Officer (DPO)

.Article 37(1) defines these organisations as: a) any public authority organisation; b) any organisation whose core activities require regular and systematic monitoring of data subjects on a large scale; or c) any organisation whose core activities consist of the processing of special categories of data on a large scale. The Regulation also allows for any member state to designate types of organisations that may also need to appoint a DPO, over and above the ones already defined.

Whilst there is no clear guidance on what is meant by "large scale" or "core activities" where an organisation is processing numbers in the thousands of records on a regular basis it would be prudent to engage the services of a data privacy specialist to undertake a risk assessment to determine the necessity of employing a DPO.

The DPO should have expert knowledge in the field of data protection and be provided all the support required to assure that this expert knowledge is maintained. He or she report directly to the highest level of management and be free from all instruction and obstruction to carry out their duties in a fully independent manner. The DPO can be an

employee of the organisation or an external contractor, however in order to ensure the independence of the role, he or she cannot be dismissed from the position merely for exercising their duties.

Some of the tasks that fall under the responsibility of the DPO are defined in Article 37. A key element of the role, aside from monitoring compliance with the legislation is the education of others processing data to meet these requirements. The DPO will also be responsible for keeping all compliance records up to date, carrying out internal audits and acting as the central contact point for responding to SARs. In order to carry out these tasks proficiently the organisation must provide the DPO with the resources necessary to do so. They must be given full access to employees and systems involved with processing data.

Another key role for the DPO is to advise on the data protection requirements of process and system development projects and taking a key role in conducting Data Protection Impact Assessments. The concept of privacy by design and by default is discussed in more detail in Section 6.1.5 and Impact Assessments in Section 6.1.6.

6.1.2. Consent

During the development of the Regulation there were extensive discussions regarding consent issues and much lobbying from companies, who will need to make considerable changes to their business processes moving forward, attempting to avoid what they saw as legislation that would be overly burdensome for companies. EU Parliament did much to represent the needs of the citizen by insisting that consent is purpose limited and loses validity when the purpose is accomplished; and consent to another use of data cannot be made a condition of a contract.

Under Article 4(11) consent from data subjects must be "specific", "informed" and "unambiguous". This is a clear inference that this should be an affirmative action, hence a move towards "opt-in" consent and away from "opt-out". There must be "explicit" consent under Article 9(2)(a) when processing special categories of personal data.

Consent must be provided for each different type of processing that occurs and under Article 7(2) the request for consent must be presented in a clear, legible format. Under Article 7(3) it must be possible to withdraw consent at any point by the data subject and

doing so must be a simple process. It will no longer be possible for organisations to demand consent for processing activities that are not strictly required to fulfil a contract, as a caveat to fulfilling said contract (Article 7(4). It must be possible for the data subject to still be able to access the contract if consent is withdrawn for the other processing activities.

The burden of proving that consent has been given will rest with the data controller who under Article 7(1) will need to demonstrate this for each processing activity. Any withdrawal of consent must also be recorded and prior to any processing being undertaken it will be necessary for data subjects' details to be compared with those flagged as having withdrawn consent for that processing activity to be excluded from it to ensure no breach occurs.

Despite broadly speaking the terms "unambiguous" and "explicit" could be seen to be the same thing, in terms of consent they are quite different. Subject of much negotiation during the four years this legislation was formed, the intention of having two different descriptions of consent was to ensure that greater effort is required to obtain consent to process special category data than ordinary data. The methods of capturing the data and consent for the two can be quite different and have an impact on the design of the instruments used to do so. Consent can be "unambiguous" without it requiring a written affirmative action to provide it; giving someone a telephone number to be contacted on for a specific reason is providing consent in this way. "Explicit" consent will most certainly require an action over and above this to ensure it meets the requirements of the Regulation, for example the use of opt-in boxes on a website.

A comparison of this would be:

1. a text box on a website asking for a telephone number for contact purposes; by adding the telephone number consent is being provided (unambiguous).
2. a text box on a website to hold a telephone number and a checkbox to activate it in order to give permission for the telephone number to be used for contact purposes (explicit).

The change in the way consent must be acquired may lead to a need to reengineer websites to ensure that visitors to the site are explicitly opting in to having a cookie file

installed on their computer rather than just having a cookies policy notification on the site. For example an organisation that has sold an item to a customer has the legitimate right to process the data for the purposes of providing that item, and any after care associated with it, plus retaining the data for legitimate financial purposes. It may also contact the customer with an offer of a similar or closely related item, under the rules of PECR, but it must obtain explicit consent during that initial offering to continue to marketing on future occasions. It may not send offers of items or services that are unrelated to the initial purchase nor may it pass the customer's details to any third party unless specific consent to do so was given by the customer at some point during the initial purchase process.

6.1.3. Enhanced Rights for Data Subjects

Under Articles 15-17 the Regulation sets out the rights of data subjects. These remain largely intact from the Directive (see Section 4.5.6 for more on this) but have been expanded to include several more. These new rights are not absolute and will depend on individual circumstances meeting the criteria.

There have been a couple of amendments to the Subject Access Request rules (see Section 4.7.2). The discretionary fee has been abolished, which may well lead to a rise in the number of requests, a cost the organisation is required to bear. The other key change is that the initial response to a request should be made within one month of receiving the SAR but an organisation can now take an additional two months if needed to complete the request.

6.1.3.1. Specific Rights for Children

The Regulation sets out the expectation for children's data to be handled with much more care. It states "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data." A child cannot consent to his/her personal data being processed. As stated under Article 8, if consent is required to process personal data then for a child under the age of 16 (this is the age requirement in the UK but this could be as young as 13 in some countries, although no younger) the consent must be sought by a parent or guardian of the child. If however there is a legitimate reason for processing the data, such as for a legal obligation, then, as with adults, no consent is required. The Regulation allows for children's data to be processed

without consent of a parent or guardian for preventative or counselling services as this is seen as a legitimate interest.

6.1.3.2. Right to Rectification and Erasure

If data is incomplete or incorrect a data subject has the right for that data to be amended and for any adverse decisions made using the incorrect data to be redressed, as stated in Article 16. Moreover, under Article 17, if data is no longer required for a legitimate reason or consent to processing has been withdrawn then a data subject has the right for data to be erased or, in the specific context of a medium such as a search engine, to be forgotten or removed from the search results. This situation already has a legal precedent in the Google v Costeja Gonzalez case (see Section 4.10.2). This is a qualified right and as such is not binding in every case.

6.1.3.3. Right to Object and Automated Decision-Making

Article 21 sets out the circumstances where data subjects have the right to object to personal data being processed if the Data Controller states the processing is being undertaken in the interests of the public or for the Data Controller's legitimate reasons. The Data Controller is then obliged to demonstrate that there are clear grounds to carry out the processing otherwise cease to do so.

Article 4(4) defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

Article 22(1) states that if profiling produces "legal effects" or "significantly affects" someone that individual has the right to object to that profiling. However, not all profiling activities can be objected to; if there is a legitimate reason to the profiling activity it may not be possible to object. Nevertheless as with the Data Protection Act, any decision based solely on automated means can be challenged.

Whilst the right to object to profiling may not be automatically applicable to online advertising, unless Article 22(1) conditions apply, which in this case could be difficult to prove, the greater need to obtain consent prior to processing should prompt a sea-change in online advertising activities.

6.1.3.4. Right to Data Portability

Article 20 sets out the rights of a data subject to obtain a copy of all personal data in a machine readable format or have that information transferred to another service provider if that is feasible. This right is only binding if the processing is being carried out by the consent of the data subject or to fulfil the Controller's contractual obligation to the data subject as stated in Article 20(1). It is not binding if the processing activity is being carried out "in the interests of the public or in the exercise of official authority vested in the Controller" (Article 20(3)).

6.1.4. Data Anonymisation and Pseudonymisation

Anonymisation and pseudonymisation of data is the process of rendering the information to a point that it is no longer possible to identify the individual that the data belongs to. There is a clear difference between the two methods of "de-identification". Whilst the Regulation does not provide a definition for anonymised data, the Oxford Dictionary has the following definition of ***anonymise***: "Remove identifying particulars or details from (something, especially medical test results) for statistical or other purposes". According to the definition in Article 4(5) "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

In practical terms the difference between the two is such that:

- it should not be possible to reconstruct anonymised data to allow individuals to be identified. The pieces of data that can lead to identification of the individual are removed from the data set altogether and deleted. This will often lead to summarised data that can be grouped together in categories. An example of this would be the number of individuals in a specific age group responding to a survey.
- it should be possible to reconstruct pseudonymised data to allow individuals to be identified. In pseudonymised data sets, the identifying factors are replaced by a random key (identifier), unique to that individual but impossible to decode by simply looking at the key. The identifying pieces of data are removed and placed in a separate data set together with a copy of the key. As required the two data sets are

then merged by matching the key in both and thereby allowing the individual to be identifiable once again.

Providing that the organisation does not acquire further information that will lead to the identification of an individual then it can keep data that it no longer requires for processing if it has been suitably anonymised. That data will no longer be bound by the data protection legislation as it highly unlikely it will pose a risk to an individual. However, there are more complex rules for pseudonymised data.

The Regulation still applies but under certain circumstances the rules are relaxed a little. If the key data set is kept separately from the pseudonymised data set and greater security measures are placed on it, (for example: encrypting the data; storing it on a standalone system; etc.) and it is only provided to those within the organisation that absolutely need it then should the data be compromised it may not require notification of a breach to the SA. If a Data Processor is only privy to pseudonymised data then, providing there is no possibility of obtaining further information that would lead to identification, it should not fall under the Regulation.

In Article 32(1)(a) it is clear that wherever and whenever possible pseudonymisation should be the norm for processing of data and should become a key feature of the development of new systems and processes moving forward (see Section 6.1.5 for more on this). Using pseudonymised data within an organisation will also act as a mitigating factor if a breach does occur and an investigation by the SA ensues.

6.1.5. Privacy and security by design and default

It is a requirement of the Regulation that organisations take seriously data protection and the risks associated with the various processing activities when creating or reengineering business processes and when developing new systems. Article 25 stipulates this requirement and outlines a few of the measures that companies can take such as data pseudonymisation or data minimisation. In order to minimise the risks involved in allowing indiscriminate access to data where it is not necessary for example, it is good practice to limit the amount of people that have access to that data or to only allow access to pseudonymised data. Other "design by default" methods would involve only capturing or disclosing enough data at the point where it is absolutely necessary to complete a task; this process of minimising the data available ensures good practice is

maintained throughout the processing activity and any breach would have limited risk associated with it.

When designing new systems data protection mechanisms should be built into the technology. An example of this would be including an algorithm to determine when a record has reached a point in its lifecycle that it should be deleted, which would also like include a system of classification of records that amends the status of each record at various points in the processing cycle. Another measure that could be put in place to ensure that records are kept as accurate as possible would be to provide a means for customers to amend their own records where feasible.

It is likely that developing capabilities in this area will take time and initially a lot of effort for organisations but the pay-off should be a reduced risk of experiencing a breach and, in the event that one does occur, the mitigating factor that proving measures were taken to reduce the risks of a breach in the decision on what penalty to impose.

6.1.6. Data Protection Impact Assessment

Privacy Impact Assessments are currently best practice and are usually the realm of big business. They are already undertaken in many large-scale and government IT projects. These are to be renamed Data Protection Impact Assessments (DPIA) and are required to be completed by any organisation where specific risks to data subjects' details may be present; more specifically where an act of processing "is likely to result in a high risk to the rights and freedoms of natural persons".

Article 35 of the Regulation offers a list of the type of risks that would trigger the need for a DPIA to be undertaken. These are defined as:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

A DPIA requires that organisations produce information flows that specifically identify who has access to personal data, when, for what purpose and how it may be transformed. It also identifies how changes to business processes might trigger a different compliance issue to those currently met, such as the need to request explicit consent for a new type of processing activity. Proof that this has taken place is likely to be requested in the event of a breach investigation and seen as a mitigating factor in the resulting decision.

The DPIA should be a recognised stage with a development project and the DPO should be consulted throughout a project on matters regarding personal data. It is usually the case that data subjects are involved in this process and are consulted in some form or other due to the perceived risk to the privacy of their data.

If the outcome of a DPIA "indicates that the processing would result in a high risk" and the Data Controller is not able to sufficiently mitigate those risks the SA must be informed prior to the processing activity being undertaken.

6.1.7. Privacy Seals and Certification

Trust is increasingly a key factor of whether an individual choses to do business with an organisation. Moving forward the EDPB and the SAs plan to introduce a data protection certification scheme that organisations can apply for to demonstrate to customers that protection of individuals' data is seen as a priority within the organisation. Whilst this has not been finalised several steps have already been taken to seek the input to this certification scheme of organisations and data protection specialists in a number of countries, including the UK. Articles 40 to 43, Section 5 of the Regulation, frame the discussion on the introduction of Privacy Seals and Certification and the bodies that will be required to oversee this standard. Articles 40 and 41 deliberate on the development of Codes of Conduct of these bodies and other professional bodies that should use either contractual elements or other instruments so as to make adherence legally binding.

The growing concerns regarding privacy amongst the general public will mean that a recognisable standard will be a clear differentiator and any organisation that holds a Privacy Seal, approved by a recognised body, and employs individuals who hold accredited certification in data protection, is likely to have a competitive advantage. As with the introduction of the British Kitemark, at the beginning of the 20th century and the

CE Mark in the 1980s, have a seal of approval over processing activities should help to raise standards generally and reduce the number of breaches suffered, particularly by those organisations who are taking data protection seriously enough to go to such lengths as becoming certified.

6.1.8. Data transfers outside the EEA

Chapter 5 of the Regulation relates to the transfer of data outside of the EEA and intercompany transfers for international organisations. As previously touched upon and as with the existing Directive, data is only allowed to be transferred outside of the EEA if a condition of adequacy has been met. These are clarified in Article 45.

Transfer to a country with adequacy jurisdiction

These are the countries to date that the Commission have found to have sufficient data protection legislation in place and no further safeguarding measures are required to take place:

> Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay

Transfer under the EU-US Privacy Shield

As has already been discussed in Sections 4.5.8.1 and 4.10.4 the CJEU ruling on the Shrems case nullified the Safe Harbor Agreement and lead to the creation of the EU-US Privacy Shield, which offers safeguards for data being transferred to US organisations registered on the scheme.

There are also ways of transferring data outside of the adequacy decisions on provision that adequate safeguards have been met. These are defined further in Article 46.

Model Clauses

As discussed previously in this report some clauses have been developed to include verbatim within a contract that will ensure the recipient of data outside of the EEA is legally bound to treat the data as if the organisation was processing within the EU, regardless of national laws.

Binding Corporate Rules

This is the case for a multinational organisation, a Data Controller transferring data to a partner or subsidiary outside the EEA should develop Binding Corporate Rules (BCRs) that ensure the safe handling of the data. Not previously recognised within the Directive as a safe mode of transfer BCRs were widely recognised by the Article 29 Working Party

as being acceptable. These have now been formally legitimised by the Regulation and are defined in some detail in Article 47.

6.1.9. Issues

A number of issues arise or are left unresolved from the adoption and implementation of the Regulation. Several of these are outlined in brief in this section.

Data Storage

Given the plethora of US cloud service providers operating in the UK and the reluctance of many to disclose the location of their server infrastructure, it made it very difficult to determine whether they were operating within the EEA or in non-EEA countries. Despite the new EU-US Privacy Shield this is still an area under question as there is a level of assumption associated with a US cloud provider operating in the EU that its infrastructure would either be in the EEA or in the US, however, without full disclosure and the ability to verify this, the servers could reside in any country outside of these agreements. The responsibility to ensure a company is within a safeguarded area lies very much with an individual as the authorities would be ignorant to the fact once Notification of data processing activities is put in place with the new Regulation.

Harmonisation of Sanctions

It will be important to ensure that the development of sanctions across the member states is standardised as much as possible to discourage organisations from shopping around to select the country with the most lenient penalties to claim as their main establishment. It is also important that a good working relationship is developed between the different member states and with the EDPB to ensure that organisations are met with the common approach and united front set out in Chapter 7 of the Regulation.

Adoption of the Police and Criminal Justice Directive

The UK has the option of not adopting of the Police and Criminal Justice Directive. If it chooses to not adopt the Directive, this will create a significantly lower level of obligation to protect data, which are for the most part classed as "special category", to the rest of the public sector and private organisations. Given that there are private companies acting as Data Processors for this part of the public sector there is a need to ensure that any of these organisations are not exempt from the stringent requirements for accountability, individual rights and penalties defined in the Regulation should national legislation in this area prove to provide reduced protection for citizens.

As well as the requirement to identify the rules regarding breach penalties as per Article 84, other unresolved issues relate to the reconciliation of the legal situation regarding the protection of personal data that is processed solely "for journalistic purposes and the purposes of academic, artistic or literary expression" as under Article 85.

Article 88 also makes provisions for differentiation between employment laws in member states.

7. Implications of UK's Withdrawal from the EU

A referendum of the UK population was held on 23rd June 2016 to decide whether to remain a member of the EU or to leave. Over 70% of the population voted and with a slim majority of only 52% the result was for leaving. This was a very divisive referendum for both major political parties with members split between "remain" and "leave" camps. Despite the Government taking a "remain" position in the campaign the Conservative party had a large number of MPs, including some Government ministers campaigning for the UK to leave. The main opposition party, Labour, also campaigned to "remain" but, although fewer in number than the Conservatives, some Labour MPs also shared a platform with the "leave" campaigners. Despite this majority of Parliament voting to "remain" the voters were just as divided and clearly appeared, for the most part at least, not to reflect the views of the MPs.

The result of the referendum has also had unintended consequences within the political parties with both facing leadership elections. The Prime Minister, David Cameron, resigned his position and after a very brief leadership contest, gave way to new Prime Minister Theresa May. At the time of writing this report there is also leadership competition underway for the Labour Party after over half of the Labour Party Shadow Cabinet also resigned citing a lack of confidence in their leader, Jeremy Corbyn.

It is likely that as time passes the cries for an early General Election (not due until May 2020), which have already started in earnest, will increase in volume, particularly so if the Government are not seen to be managing the withdrawal from the EU very well.

7.1. Invoking Article 50 of the Treaty of Lisbon

Before any formal arrangements can be made to pull out of the EU, the Government of the UK is now required to invoke Article 50 of the Lisbon Treaty which states that "Any member state may decide to withdraw from the union in accordance with its own constitutional requirements.

Article 50 does not state when it should be invoked but does require that once it has been, the Government will have two years to conclude the negotiations regarding the terms of withdrawal. The procedure for the negotiations is set out in Article 218(3) of the

Treaty of Lisbon, which will take place between the UK Government and the EU Commission, who will conduct discussions for and on behalf of the EU member states. Any extension of this negotiation period will need to be agreed unanimously by all the remaining member states.

The outcomes of these negotiations will have far-reaching consequences for many areas of life in the UK, such as the economy, cross-border security, migration and immigration, higher education, and research and development. They will also have implications for the remaining EU member states whose citizens work in the UK, come to the UK to study, sell to or buy goods from the UK or have investments in UK financial instruments. It will no doubt be a very difficult period of extrication for all concerned and will take careful consideration of the impact of each decision on future relations for all parties.

7.2. Reviewing Legislation

Along with many decisions that will need to be taken with the EU there will also need to be a substantial effort to review the legal situation in the UK. This will involve repealing, or as a minimum amending, the European Communities Act 1972, the piece of legislation that designated the primacy of EU law over UK national law.

It is a relatively straightforward issue with EU Directives as to affect these into law national legislation will have already been designed and adopted to meet the objectives set out. However, with Regulations this is a different matter. An EU Regulation is the instrument that enacts the law in the member state therefore the UK Government will need to decide which Regulations it wants to keep and which it wants to reject. By some estimations there are over 40,000 pieces of legislation that have come out of the EU. These include regulations, directives, decisions and verdicts from EU courts that may affect any number of things from local laws to trade agreements and international treaties. Each must be considered fairly carefully as every piece of legislation will have some consequences to a lesser or greater degree.

There are several possibilities for the Government to deal with the laws.

7.2.1. Adopt All Previous Legislation

The first option is a rather simple one that would generate the least amount of immediate repercussions and that would be to pass an Act of Parliament that enacts en bloc all of the pieces of legislation relating to the EU that have gone before. However, this type of extreme measure is unlikely to happen given that one of the key reasons for calling the referendum in the first place was to give a voice to the portion of the population that felt disaffected by the degree of influence the EU has had over UK laws. There is also very likely to be conflicting political pressure from the left and right wing Parliamentary parties, and groups lobbying on behalf of citizens and businesses to repeal legislation that either sees as draconian or stifling, to prevent a bill such as this to be passed.

7.2.2. Appoint Legislative Advisory Groups

A list could be compiled of pieces of legislation that each of the Parliamentary parties and various interest groups believe to be vital to avoiding economic collapse, could cause exclusion from international agreements or present a risk to national security if not adopted. These could then be scrutinised as a priority in parallel by an assembly of legal and constitutional experts in the specific field of the legislation under consideration. Ideally these would be specially selected to represent the views of the various factions and should be given a remit to propose any minor amendments before presenting the bills to Parliament for Royal Assent.

Anything requiring any major amendments would need to be deferred to Parliament but given the consequences of not carefully considering all the laws prior to the 2-year period activated by invoking Article 50, the number of bills subjected to the usual lengthy process of Parliament should be kept to the barest minimum.
Attention can then be turned to the legislation deemed to have less of an impact on international relations and therefore deemed to be of a lower priority. It will likely become clear over the course of this activity which EU laws should be kept or rejected, to ensure the UK remains flexible enough to react to international opportunities whilst protecting the rights and values of citizens.

7.2.3. Convene a Special Parliamentary Group

An alternative solution and perhaps the most likely to happen is for the current Government to assemble a group of ministers and constitutional experts from within its ranks to select the pieces of legislation that it deems to be the most important to pass

into law and do so with as little Parliamentary scrutiny as it can in order to speed up the process.

This approach is likely to be the most effective way of passing legislation from a time perspective but much more likely to provoke a negative reaction from the members of the public. Given the division across party lines between the voters this approach could be seen as an opportunistic move by a political party working to serve their own interests rather than those of the majority of citizens.

One thing that is very evident is that in order for this process to be successful it would need to be conducted in the most democratic and transparent of manners although the very nature of its constitution would suggest that the interests of some groups of society would be underrepresented.

It is true that any laws that are enacted can subsequently be repealed but not easily and not without some possible fallout from the process.

7.3. Options for Data Protection

One legal issue that will need resolving rather quickly is that of data protection legislation. As with all member states of the EU, until the Regulation legislation comes into force on 25th May 2018 then all laws that were created by each Government to enact the Directive in the member state will still be law. In other words, the Data Protection Act 1998 is still the primary legislation in the UK. It is what happens once the Regulation is activated that needs some thought and given the complexity of the compliance framework, UK organisations and any overseas companies sharing processing with them will benefit from having as much time to prepare as possible.

Assuming that Article 50 is not invoked immediately and that a full 2-year period will be needed to conclude negotiations, despite the reassurances of an ICO spokesman in a statement made on the day the results were announced that "reforms to data protection law would not directly apply to the UK" (ICO 2016) if we were no longer going to be part of the EU, there is likely to be an overlap period of several months from its adoption by other EU member states before the UK's official withdrawal from the EU. Without some clarification of the situation there will be a legal "grey area" for organisations within the

UK if it is not clear as to whether the new rules do apply, which could end up being a costly risk for organisations to take if challenged and lost in the courts. The ICO spokesperson did concede that "if the UK wants to trade with the Single Market on equal terms we would have to prove 'adequacy' - in other words UK data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018." Regardless of the legalities of the situation during the overlap period, there will be significant difficulties moving forward should the UK fail to act on this advice and introduce safeguards equivalent or superior to those offered by the Regulation.

It will take considerable effort for UK organisations to prepare for the coming changes for such a brief period of time. It stands to reason then that a decision will need to be made soon on the type of data protection reform we wish to implement, to ensure that the effort made is worthwhile and actually moves towards conformity with other nations rather than being a failed exercise costing time and money; something that particularly needs to be avoided in such turbulent economic times. As the ICO emphasised in its statement, it is essential that consistent data protection regulation exists internationally as "many businesses and services operate across borders and cooperation is required if we are to provide a suitable business landscape and regulatory framework to allow a thriving and global digital economy to flourish.

Given that there are over 2 million EU citizens currently living and working in the UK, and this is likely to be the case moving forward, there is no easy way for an organisation to avoid processing the data of one of these citizens without discrimination. It will therefore be necessary to abide by the Regulation in a similar way at least to non-EU member states that have made specific agreements with the Regulation, such as the US, or have been vetted by the EU and deemed to be a "Safe Country" for the purposes of the new legislation. Any rules introduced into law by the UK Government or any agreement entered into will very likely need to meet the same "adequacy" test they have each had to undergo.

In her speech at the Privacy Laws & Business Annual Conference on Data Protection (July 2016) Baroness Neville-Rolfe DBE CMG, Minister for Data Protection, reinforced the view that having adequate data protection in place will be a "major consideration in the UK's [post-Article 50] negotiations going forward." She stressed the likelihood of the implementation of very similar legislation being adopted in the eventuality that the UK

does not adopt the Regulation as "we will still need to develop policies to meet the same problems. The answers will need to draw on the same facts and needs. So while the detailed future may be different from what was envisaged [pre-referendum] the underlying reality on which policy is based has not changed all that much."

There is also the issue of the new EU-US Privacy Shield agreement and what the situation would be regarding the UK. At the time of writing this report the proposal for the safe transfer of EU citizens' data to the US was still being debated by EU officials and UK delegates from the Department for Culture, Media and Sport were present in the final negotiations but, as Baroness Neville-Rolfe stated "we will need a satisfactory understanding with the US of the rules [of the EU-US Privacy Shield] to be applied [to the UK]. The final agreement is expected before the end of July 2016.

It would be a useful exercise to see just how the "Safe Countries" legislation compares to the Data Protection Act 1998. It could be the case that the DPA as it currently stands offers greater protection than one of the countries on the "Safe" list and therefore could be argued that in order to cooperate with EU countries moving forward no reform of the current law would be immediately necessary. However, in the current, somewhat acrimonious, climate created by the decision to leave and the impact this is going to have on the other member states, it is unlikely that the EU would see this as a favourable option. If proved however, it could be agreed that discussions on new arrangements surrounding cross border data processing and handling of EU citizens data be postponed until after the more pressing constitutional matters are resolved, which would benefit all parties in having to undergo further negotiations that could be done at a later date.

The simplest solution of course would be to seek agreement with the EU that if the Regulation was implemented in its entirety into UK law the matter would be resolved. It would also be an effective solution to expand the EU-US Privacy Shield agreement to include the UK and given that UK representatives from the EU were involved in the talks throughout the negotiation process it would be appropriate to allow this to happen. Given the impossibility of separating out the data of EU citizens who live in the UK from that of UK citizens, it would show that the EU is serious about safeguarding its citizens' data regardless of where they reside. This would also be a step further towards a global agreement on data protection, which should ultimately be the goal of all nations participating in global trade of goods and services.

In light of the revelations of Edward Snowden that the GCHQ is just as actively collecting and storing US and EU citizens as the NSA is, it seems likely that this may also become a factor in the data protection discussions. There are some challenges currently being made in the UK and EU courts regarding the actions of the GCHQ; the outcomes of the cases may have some consequences and influence on this debate. The upcoming Investigatory Powers legislation currently working its way through the UK Parliament could also prove to be a bone of contention with the EU and how safe it views the UK moving forward.

It is estimated that over 60% of internet traffic crosses the Channel as it is routed indiscriminately from one access node on the internet to another (both of which could originate in the same country but pass through different jurisdictional areas before reaching the destination) flowing from the EU member states to the UK and vice versa. This system of random routing is the very essence of how the internet works and it would be an extremely difficult, costly and lengthy process to fundamentally change the way that traffic is routed between the UK and the EU. The solution would require the development of a "walled garden", an approach to data management akin to an Intranet (an internal network with restricted access). This would consist of a fragmented data network where the nationality of a person would need to be established prior to any processing taking place. This could threaten the notion of anonymous access of the internet. Data centres would need to be created within the EU and the EU member states would have to insist on the global organisations operating within their borders to not transfer any data to the UK. There would also need to be a solution put in place for the EU countries to transfer data to the US if it wishes to avoid routing traffic through the transatlantic pipelines located in the UK.

8. Local Authority Compliance

The Government are keen to move as many public services online as they can, in an attempt to save money. However, in doing so this poses many risks for a sector that has been dispensed some of the largest fines in the UK for data protection breaches, despite legislation having been in place in the UK since 1984. With an increased number of breaches occurring through online access to data there is a real risk that the number of breaches will increase. So far, reporting these breaches has been voluntary for public sector organisations, except central government bodies and the NHS but this will soon change. With the new Regulation comes mandatory breach reporting so it is almost inevitable that the amount of fines will consequently increase. Any increase in fines will certainly hurt frontline services already struggling to provide a good level of service in the current climate of decreased spending for Local Authorities (LAs) by the Government.

One way to safeguard against this is to improve the compliance regime within the public sector. LAs should increase awareness of legislation and put robust policies in place that promote and encourage best practice amongst employees. Many of the rules that determine how a LA should behave and the types of procedures it should put in place are defined in the Local Government Act 2000. This law is discussed further in this section.

This section of the report will focus on the specific area of local authorities in England and in particular their responsibilities and procedures relating to data protection and highlight the potential consequences of failing to comply with the legislation.

8.1. What is a Local Authority?

A local authority (LA) (also known as local government) is an organisation responsible for delivering some services on behalf of the central government to members of the public living in a clearly defined geographical location. As power has been devolved to the Scotland Parliament, the National Assembly for Wales and the Northern Ireland Assembly, decisions on how local authorities act in Scotland, Wales and Northern Ireland and what services they are responsible for delivering locally consequently lies with these institutions. However, as there is no separate Parliament or Assembly specifically for England, legislation relating to the governance of local authorities in England is decided by the UK Parliament.

Exclusions

As discussed at the outset, this report focuses on English Local Authorities and any differences between these and those in other UK jurisdictions are outside its scope; this is a topic for further research. It is also recognised that National Health Trusts are also deemed to be a form of local government with devolved powers from central government for spending on all services, employment, equipment, buildings and other assets related to health in the UK for hospitals, clinics and GPs. Specific data protection requirements for the NHS are also outside the scope of this report and the topic merits separate research. As it has a separate and distinctive legislative structure to the rest of the UK the City of London is also excluded from this report and its findings.

Structure

England is divided into 9 geographical regions: London; East of England; East Midlands; North East; North West; South East; South West; West Midlands; and Yorkshire and the Humber.

There are nearly 400 local authorities in these regions and they fall into 2 categories, single and two-tier.

- Single-tier authorities: these authorities provide all the local services to citizens in their areas.
    - Metropolitan and County Boroughs
        - Cemeteries; consumer protection; council tax collection; education; fire; housing; libraries; licensing; parks and gardens; planning; police; social services; transport; waste collection; waste management.
    - Unitary and Shire Authorities
        - Cemeteries; consumer protection; council tax collection; education; housing; libraries; licensing; parks and gardens; planning; social services; transport; waste collection; waste management;
        - Fire and police (Shire Councils).

- Two-tier authorities: the provision of services in these authorities is split between County and District level organisations.
    - County Councils (upper)

        - Consumer protection; education; fire; libraries; police; social services; strategic planning; transport; waste management.
    - District Councils (lower)
        - Cemeteries; council tax collection; housing; licensing; local planning; parks and gardens, waste collection.
    - Greater London (upper)
        - Fire; police; regional development; strategic planning; transport.
    - London Boroughs (lower)
        - Cemeteries; consumer protection; council tax collection; education; housing; libraries; licensing; local planning; social services; waste collection.

In addition to these there are also around 10,000 Parish and Town Councils, primarily situated in rural areas. The services they are responsible for providing vary but mainly consist of those such as libraries, community centres, leisure facilities, parks and gardens and the like.

Some smaller authorities collaborate through "Joint Boards", to provide some upper tier services such as fire and police, public transport and waste management across authority boundaries.

Legislation was passed in 2000 intended to rationalise the political structure of LAs, which were deemed to be too slow to respond to required changes. At the passing of the Local Government Act 2000 the old committee approach to decision making was replaced by one of four types of executive structures, to be chosen by each LA. These options were:

1. an elected Mayor plus an elected cabinet of 2-10 councillors;
2. an elected Council Leader plus a cabinet of 2-20 councillors, selected either by the Leader or the full council;
3. an elected Mayor plus a Council Manager, an officer appointed by the Council; or
4. District Councils with populations less than 85,000 could select a revised version of the committee system previously employed. This option was also available to those areas where it was deemed to be more suitable than the other options.

One LA selected option 3 and a handful option 1 and 4, but the majority chose an elected Council Leader supported by a cabinet system. A number of LAs, however, have since returned to a Committee-based system since the passing of the Localism Act 2011, which, although criticised by some as being inapt, was created to facilitate the transfer of powers from central Government to regional decision makers.

All LAs have a Constitution, which should be made publicly available. It describes the decision-making structure of the LA; the limitations of its power; the responsibilities of the leaders; the procedures it follows; and the rights of the citizens.

In 2012 when the Regional Development Agencies, previously responsible for the distribution of Government funding on matters including trade, business, skills, employment, culture, and environment, were abolished, some of the functions of these organisations were again centralised which has caused some criticism of the Conservative Government seen by some to be reversing the process of devolving power to the regions.

According to the UK Labour Market: June 2016 survey carried out by the Office for National Statistics, there were just over 4 million employees working in the public sector in England, which represents just under 16% of the English workforce. This figure includes employees of central government offices and NHS workers but excludes GPs (who are classed as self-employed) and university employees, both academic and non-academic (who are classified as working for a Non-Profit Institution Service Households). It also includes Royal Bank of Scotland employees who, since the collapse of the financial markets in 2008 and the subsequent buyout of the bank have been reclassified as public sector workers.

8.2. Data Protection Responsibilities

Local Authorities are no different to any other organisation managing personal data, they are expected to comply fully with the DPA. Guidelines on the types of policies and procedures to put in place are issued by central government from time to time but, unlike central government offices and the NHS who are expected to follow much stricter rules regarding the protection of data, it is up to individual LAs what types of measures they put in place to safeguard citizens' data, providing of course that they meet the obligations

set out in the DPA. However there are a number of guidance documents and tools developed by the ICO specifically to aid LAs cope with the particular issues that they face; these will be discussed in more detail later in this section.

The type of data held by a particular LA will depend on the services it provides. However, it is highly likely to be classed as "Sensitive" data for the DPA or "Special Category" for the Regulation. As well as names, addresses and dates of birth, there is likely to be a raft of other information that different departments of an LA hold. Some of the more common types of data held are:

- financial details relating to payment of council taxes, rent, library charges, etc.;
- special needs and health requirements relating to social services, education, housing, transport, etc.;
- criminal records and debt management;
- education records;
- family circumstances relating to births, deaths, marriages, civil partnerships, divorces; and
- any involvement with family and social services.

8.2.1. Data Sharing

Many LAs share data with each other as a matter of course. As with sharing data with a sub-contractor, there is a risk involved in transferring data from one organisation to another and this needs to be taken into account by any LA who does so. There are a number of factors to consider and steps to take to ensure continued compliance with the DPA.

- Be transparent with the data subjects about who the data is going to be shared with by adding this to the Information Notice.
- Have a shared data retention policy if data is simultaneously stored in different places to ensure that if it is deleted in one location, it is also deleted in the others.
- Ensure that adequate security measures are put in place for the transfer of the data, such as encryption, and storage of the data at its destination, e.g., secure databases with restricted access to the data. If it is to be transferred overseas care needs to be taken as to what country it either transits through or is processed in. This also includes the use of any cloud services; an LA should refuse to contract any cloud

service where the provider is not willing to disclose the location of its servers or provide access to the LA to do due diligence on the contract.

- It is also important to have a shared SAR process so that all parties sharing data know who will be the primary contact when dealing with any request for information and to ensure that all data stored in numerous locations is fed back to that contact for disclosure to the data subject.

Pseudonymisation is one method of ensuring that the data can be shared without compromising the privacy of the individual. This type of method is used in data mining techniques such as classification and profiling in order to predict the likelihood of particular outcome occurring for someone with similar characteristics to the anonymised individuals. It is recommended that the public sector use pseudonymisation techniques wherever possible when sharing data with sub-contractors and other LAs that do not need to know the personal details of individuals to complete the processing activity they require the data for. The anonymiser key (often a series of numbers or numbers and letters) should be kept separate from the data set and only be used when needed.

Providing that no individual can be identified through the data set, pseudonymisation will in most cases discharge the third party who shares this data set from any data protection obligations as it is not likely to cause any harm to anyone if it is misused.

8.2.2. FOIA and DPA Intersection

As already mentioned in the section on related legislation above, all local authority organisations have a duty to respond to requests for information relating to business activity, under the FOIA 2000, as well as having to respond to requests for information held on individual data subjects, SARs, as specified in the DPA 1998. For the purposes of this report FOIA requests and the handling of information that would be deemed to be eligible for disclosure under the FOIA will not be discussed, as compliance with this piece of legislation is a rather large topic in its own right. However, it should be noted that these two types of data do overlap in certain circumstances and any FOIA requests should be handled very carefully in these situations so as not to inadvertently breach the DPA whilst attempting simultaneously to comply with the FOIA.

An example of this would be if a request was made for information leading up to a decision being made by the LA that was influenced by members of the public. Allowing

details of any individual to be released to the public in an FOIA request, without the explicit consent of the individual would be a breach of the DPA if it was possible to identify the individual from the information provided. Personal details would usually be redacted or removed before any information is made public, unless the identify of involved individuals is already known or despite the redaction of details it is still clear who the individual is. There are a number of exemptions and exclusions such as this pertaining to the disclosure or non-disclosure of personal details in a variety of circumstances and any FOIA requests should be handled by someone who has a very good understanding of how to comply with this law.

It is also pertinent to be aware that under Section 95 of the Local Government Act 2000, unauthorised and wilful disclosure of information could lead to a term of a maximum of two years imprisonment, although this type of punishment is quite rare.

8.2.3. Data Classification

In October 2013 the Government's Cabinet Office Security Classifications Policy was introduced, and came into force in April 2014, to provide a standard means of classifying the various types of data processed by government bodies. The guidelines describe how local authorities should label specific types of data they are processing and what management measures each "class" of data requires.

There are 3 types of classifications:

- Official
- Secret
- Top Secret

There is no need for public sector organisations to routinely classify documents it produces as *Official*. According to the guidelines set out in "FAQ Sheet 3: Working with Personal Information" (UK Government 2013) the following is stated for the handling of personal data:

> *"Almost all personal information/data will be handled within "Official" without any caveat or descriptor. In very limited circumstances, specific sensitivity considerations may warrant additional (generally procedural) controls to reinforce the "need to know" for access to certain personal data at "Official".*

Personal information / data should only be managed in the "Secret" classification where the context warrants defending against a heightened threat profile, e.g. data identifies a person as being in an exceptionally sensitive position or situation (e.g. an employee of the Security and Intelligence Agencies)."

The classification of documents allows public sector employees to see quite clearly the type of content contained within a document without having to read it or have specialist knowledge of how to interpret the information imparted in it. It offers an extra level of security around disclosure of extremely sensitive information. However, given that the majority of information that is classified will be deemed "Official" this actually means very little in most organisations and circumstances. The system of classification will only really be effective in those situations where it is usual to encounter "Secret" and "Top Secret" information. The LocalGov organisation state that the greatest benefit to having a classification system is that "By putting the classification obligation in the hands of staff at all levels, you effectively draw them into an active role in data security, which provides a greater defence against the loss of sensitive information."

8.3. Policies and Procedures

It is necessary for all organisations to have well-known processes in place so that employees are aware of what is expected of them and they are able to routinely output consistent products and/or services. LAs are no different in this respect but as well as having clearly defined methods to follow to fulfil routine tasks they also have to comply with the rules and regulations set out by government. In order to comply with the DPA there are a number of key policies and procedures that any LA should adhere to as a minimum.

Data Controller Notification

All LAs need to register as a Data Controller with the ICO. If a LAs has more than 249 employees the registration fee to pay is £500, otherwise it is £35. The ICO website guides a Data Controller through the process of registration and makes suggestions on the types of processing activities and data subjects a specific organisation might have depending on the organisation type selected. These suggestions can be edited to ensure the registration is accurate. If a Data Controller requires help with the registration he/she can request support from the ICO rather than risk completing the registration incorrectly.

Registration must be renewed each year and any time there are any changes to the processing activities or the groups of data subjects the registration must be amended. Failure to register or keep a registration up to date is an offence.

Employee Data Protection Training Schedule

The key to any successful data protection compliance starts with individuals who are fully informed of their responsibilities. In order to do this it is necessary to provide a comprehensive training programme that, as well as providing them with a full understanding of the law and the consequences of not complying with it, takes into account the role of the individual, the types of data they will encounter and how to minimise the risk of causing a data breach.

Breach Notification Policy

Despite all the best endeavours to avoid a data breach there is a high probability that one may happen. It is therefore very important that all employees know exactly what constitutes a breach and what do to in the event of one occurring. It is useful to have a list of situations, such as faxing a document to a wrong number, losing a flash memory stick, theft of a laptop, etc., and what the steps should be to take if any one of the situations occurs. There should also be a clear policy relating to online products such as websites, databases, intranets, etc., in the event of unauthorised access. Data breaches are discussed in more detail further in this section.

IT User Policy

Whilst individuals are always to be held responsible for their actions online, it is the responsibility of the LA to provide employees with clear guidance on what is and is not acceptable behaviour when using IT equipment and services provided for business use. For example, it must be made clear that under no circumstances should any employee disclose the details of any other employee or citizen via social media or email. The organisation may also wish to limit how employees can use LA systems for personal online use or forbid it altogether in order to reinforce clearly the need to keep business data separate from an employee's personal data. It is common for IT departments to limit the users' ability to install programs on PCs to lessen the possibility of introducing a virus on to the network but it is worth reiterating the need to use common-sense when opening attachments in emails and exercising caution to avoid being deceived by social engineering techniques.

A high risk scenario for data breaches is the use of portable devices however these are becoming much more commonplace and will no doubt continue to be popular as more data is moved online and flexible working is encouraged. It is therefore extremely important that clear information on the use of laptops, particularly off premises, and smartphones should be included in the IT usage policy. The policy should have a section on the use of employees own devices (commonly known in the IT industry as Bring Your Own Device or BYOD) for work purposes. This should include instructions on how to access work related data, encrypting data and remote wipe facilities in the event of a loss of the device.

Contracts with third parties

The rise in outsourcing in the public sector poses a growing risk for data protection as the number of people able to access data increases and data is transferred and stored on a variety of systems in different locations.

According to Public Sector Executive (2016) outsourcing by the public sector is rising and that local government "spent £756m on outsourcing in 2015, with the total value of contracts signed by councils up 23% year-on-year" with the average value of contracts growing by 30%, according to a study conducted by Arvato and NelsonHall. The study cited new demands to make savings due to major welfare reforms, and the desire to transform services, as reasons why they believe the appetite for outsourcing will continue to increase over the next few years. Debra Maxwell, Arvato's CEO for CRM and Public Sector said that the business process outsourcing organisation expected to find the public sector bodies looking for "new approaches to transformation in 2016, such as moving services entirely online, sharing services virtually, and introducing robotic process automation. Private sector partners will continue to play a key role by bringing in expertise and technology to help make those changes." The study cited the areas that are seeing the greatest pace of privatisation and outsourcing are the justice, healthcare and welfare domains with most councils mainly procuring HR, revenues and benefits and multi-process customer services.

This picture reaffirms the trend outlined in a study in 2014 by Information Services Group (ISG) consultancy reported in the FT.com. They stated that the amount of public money spent on outsourcing has doubled to £88bn since 2010 compared to £45bn spent in the previous 4 years before the coalition government imposed spending cuts on the public

sector. Luke Mansell, a partner at ISG, said the company expected growth in the public sector to continue.

This increase in the use of Data Processors unless handled correctly may lead to issues with data protection. It does not diminish the responsibility of the LA to ensure data is processed according to the DPA. It will be essential to have contracts that include data protection responsibilities and define the rules such as those for sharing data, discussed in Section 8.2.1. Any company carrying out processing activities on behalf of a LA should allow the LA to audit the processing and demand any shortcomings in the managing of personal data be rectified forthwith. There are model clauses available on the ICO website that can be used in contracts. However, given the greater need for accountability and proof of compliance where public funding is financing the service, it would be prudent to ensure any contracts are administered by legal experts.

Information Notice

To comply with the transparency obligations set out in Principle 1 of the DPA, every organisation must have a Fair Processing (or Privacy) Notice (as described in 4.7.1 section), and this is no different for LAs. The Notice should contain clear information about what types of data the LA process, how it processes it, which third parties it is likely to share the data with.

It is good policy and best practice to have a copy of the Privacy Notice on the website and for any electronic correspondence with individuals whose data is to be processed to include a link to the site notice. It is also necessary to send out a printed copy of the Privacy Notice with all written correspondence to an individual.

As with all situations where a data subject has an option for his/her data not to be processed, an opt-out solution must be provided. In the context of written communication this may include a form that can be completed and returned to the LA or simply be the contact details on the person/department in the LA responsible for removing the data subject's details from the processing activity. To provide the same service online a series of web-based forms can be developed and the data subject directed to the relevant form.

Subject Access Request policy

As discussed in Section 4.7.2 above, all data subjects have a right to copies of their personal data held by any organisation, barring any exemptions from disclosure. LAs

should comply fully with this obligation but, as explained previously (see Sections 8.2.1 and 8.2.2) care should be taken to ensure no one else's privacy is compromised, including that of the employees of the LA in complying with a request. Third party contractors and partners in data sharing processes should be part of the procedure put in place to ensure all data is included in responses within the time frame allowed.

Risk Management Procedure

All organisations that take corporate governance seriously will undertake regular risk assessments and maintain a risk register that can be used to mitigate any issues should an occasion arise where external authorities conduct an investigation due to an event occurring. This is no different in local government. There are a number of best practice guides on corporate governance in LAs to help improve risk management and procedural compliance but, while the Local Government Act 2000 sets out the framework of behaviour expected, there are no statutory guidelines binding LAs to behave in a particular way. As has already been discussed previously in this section LAs have a significant amount of autonomy to determine how they achieve their objectives, providing they adhere to laws of the land and remain true to their Constitutions and accountable to the authority structure agreed upon. However, if only in order to ensure re-election, LAs should always be striving to improve the level of service provided and the sharing of best practice is one way to do so.

It is highly unlikely that a LA does not have a risk management strategy in place so making the assumption that all do, it will be necessary to add data protection objectives to the risk register if they do not already exist. This consists of assessing individual areas of the organisation where data might be at risk, assessing the likelihood of a breach occurring and what the potential impact of that would be. This is then followed up by identifying a course of action in the event of a breach occurring and putting measures in place to minimise the risk.

Amendments or new entries should be made to the register when there is a change in the risk. This could be for a number of reasons:

- the development of or reengineering of a business process involving processing of personal data;
- the development of or reengineering of a IT system to process personal data;

- the appointment of a sub-contractor or outsourcing company who will have access to personal data;
- the awareness of a new threat to data security; or
- as a result of a data breach.

8.4. Data Breaches & Notification

All central government bodies and the NHS Trusts across the UK have been mandated by the Government to report any data breaches that could pose a risk to an individual's privacy if misused. However reporting breaches is currently still a voluntary procedure for LAs.

The key incentive for notifying the ICO of a breach is that it is seen as a mitigating factor when the ICO is considering the penalty to impose on an organisation. Therefore, it is in the interest of an organisation that has experienced a breach that could impact on the privacy of an individual to report the breach to the ICO, as the act of disclosure could result in reduced penalties.

Whilst there is currently no legal requirement in the DPA to report a breach, the Human Rights Act 1998 (HRA) does provide a right to privacy in law so it could therefore be argued that if a data breach where the privacy of an individual was at high risk was ignored that would in fact be violating the HRA and therefore be illegal. In the event of a Section 55 (DPA) breach, which relates to obtaining and using personal data illegally, there is no legal recourse for criminal prosecution of an individual that is likely to lead to a custodial sentence. Prior prosecutions of Section 55 crimes have led to individuals losing their employment, being issued with a fine or simply being issued with a warning. Many parties are calling for greater punishments and the potential to receive a custodial sentence to provide a greater deterrent for individuals to misuse the level of trust placed in them.

This absence of stricter guidelines on what constitutes a breach and when (and if) one should be reported has led to a varied attitude to compliance and approach to enforcement across the country as can be borne out by surveys carried out by, amongst others, the ICO and Big Brother Watch, an independent oversight organisation that

campaigns to protect the civil liberties and privacy rights of individuals. The findings from these studies are discussed in more detail in Section 9.1.

All studies highlight the fact that there is a problem within local authorities across the country and there are many incidents of breaches of the DPA. However the picture varies significantly from the private to public sectors and from authority to authority. This could be due to some organisations simply not reporting breaches. As well as running the risk of incurring a fine from the ICO a breach in a private company could affect the reputation of the business resulting in a loss of customers thus revenue. In the public sector customers cannot vote with their feet and simply choose another provider so there is no risk of this; there will still be the same amount of people requiring the same services. The true risk in the public sector is of a fine that could affect the amount of money available to fund frontline services. It is likely that high value fines impact on the quality of service that an LA can deliver and this may be the reason some choose not to report breaches.

9. Findings and Recommendations

This section looks at the current culture of data protection compliance within LAs in regards to areas that may require attention and the changes that will need to take place within these organisations in order to meet the obligations of the new data protection legislation.

These findings and recommendations make some key assumptions regarding the situation arising from the UK Referendum decision to withdraw from the EU:

- There will be a period of overlap where the UK is still a member of the EU and the new Regulation will become law.
- New data protection legislation will be implemented in the UK.
- The new legislation to be implemented will be identical to the new Regulation.
- The UK will negotiate an agreement to join the EEA as per Norway, Iceland and Lichtenstein, and will therefore be included in the agreements for:

    - the "One Stop Shop" to regulation, resolution and reform;
    - the EU-US Privacy Shield data transfer scheme.

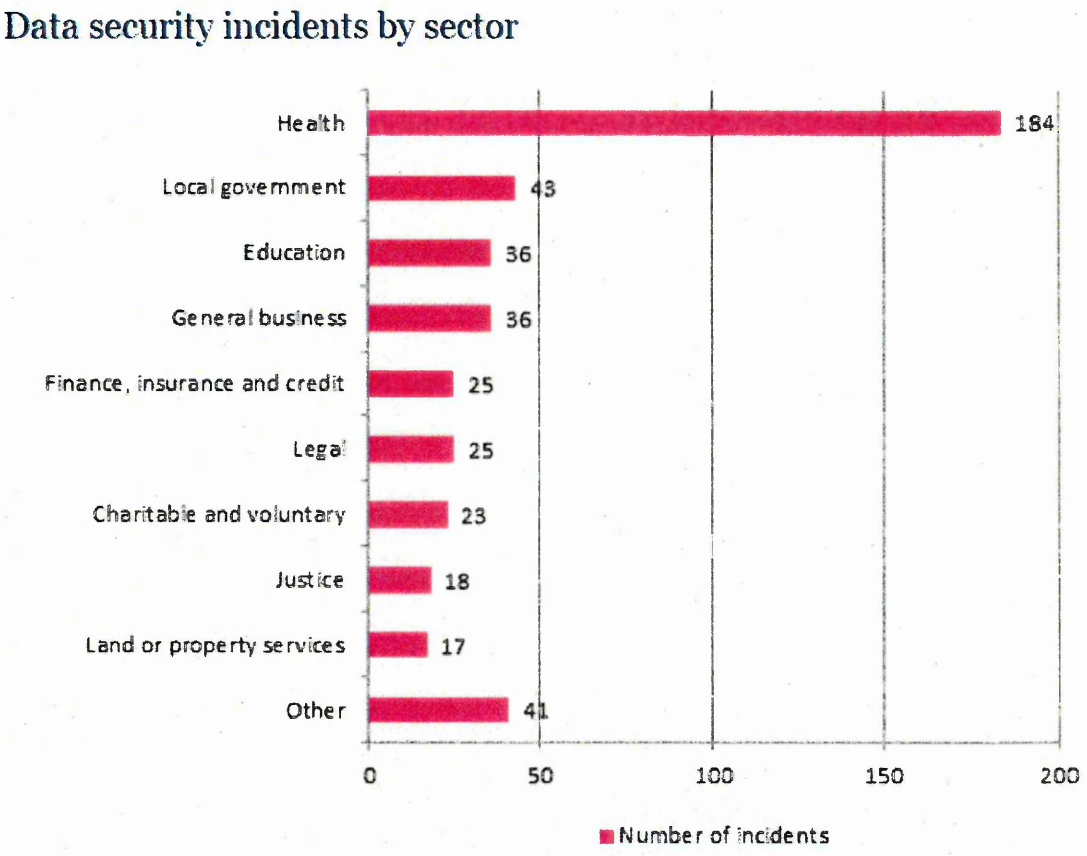
In other words the assumptions made in this section of the report are that the situation regarding data protection legislation pre and post withdrawal from the EU will remain the same.

The above assumptions do not include the situation with the Police and Criminal Justice Directive as given the UK will no longer be a signatory of the Lisbon Treaty the Article 10 opt-out of this area of legislation and EU judicial oversight will no longer be valid and will therefore need to be renegotiated so that partial powers can be passed to the EU in the area of data protection. This will need to be discussed as a separate matter and is outside the scope of this report to speculate on the potential outcomes. What is certain is that the factions within the EU that are not in support of the UK's withdrawal from its membership will not allow the UK to obtain all of its demands in the negotiations lest this set a precedent for other countries to follow suit. Thus, some concessions will need to be made on the part of the UK to retain access to the EU common market and facilitate the transfer of data for international organisations.

9.1. Current Breach Reporting

According to the latest summary of data on the ICO website of the breaches reported during January to March 2016 there was a 10% decrease from the previous quarter. However, the total number of cases in this quarter across all business sectors still amounted to 448. The data showed that the highest number of reported breaches came from the Health sector, at 184. However the ICO acknowledge that this it is not a surprising finding given the sensitive nature of the personal data in that sector and the mandatory requirement to report breaches.

How the rest of the figures are distributed can be seen in the chart below, taken from the ICO website.



Data Security Incident Trends by Industry Sector, Jan-Mar 2016, Information Commissioner

It is not immediately clear from this chart exactly how many of these breaches have been reported from LAs as some ***Education*** will also fall under "Local government" and others under "General business" depending on whether the institution is still under control of the Local Education Authority or has converted to an Academy or Free School.

To complicate matters further, the groupings in the raw data accompanying the results are not the same as those (above) published on the website and include a breakdown of "Other" that includes organisations such as those in the "Retail and Manufacturing" sector (that arguably should be considered to be part of the "General business" sector; there is no discussion as to why this is not the case) and those in "Central government". It is therefore unclear exactly which of the organisations in a number of the other categories would belong in the private sector. There is also an "Other" category remaining after the breakdown.

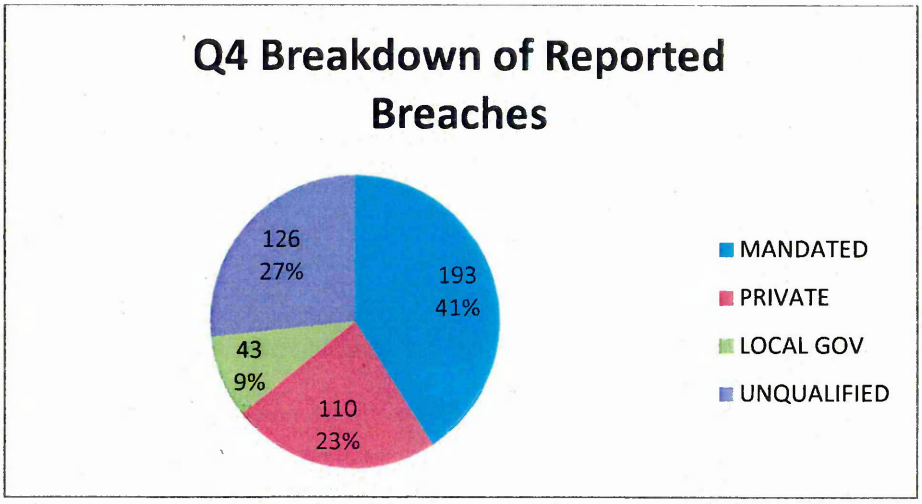
In an attempt to make a clearer picture of the figures, the raw data was recompiled as below. The sectors that were ambiguous in terms of whether they were part of the private or public sector were labelled as "Unqualified" in the figures. The other sectors were then separated into those public sector bodies that are mandated to report breaches, the private sector and the public sector not required to report breaches. (See Appendix 2 for raw data sets).

Label	**Sectors**
Mandated	Central government, Health
Private	Finance, insurance & credit, General business, Retail and manufacture, Utilities, Land or property services, Legal, Marketing, Media
Local Gov	Local government
Unqualified	Education, Charitable, Justice, Members, Online Political, Regulators, Religious, Social Care, Transport & Leisure, Other

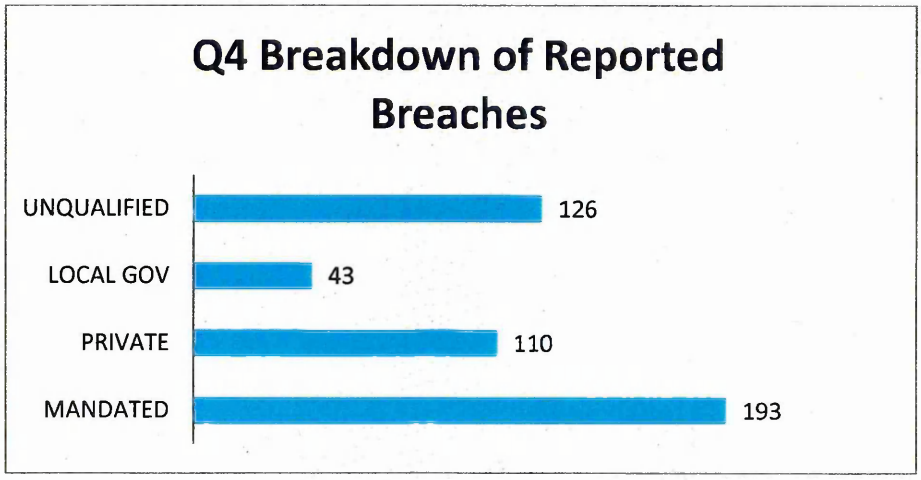
There were also some discrepancies in the ICO raw data set. The Total below represents the manually entered number in the Total column in the raw data set provided. The Actual Total represents the calculated sum of the number of entries in each data breach category. As can be seen from the figures, Quarter 1 figures tally accurately however Quarters 2 and 3 are missing entries in the raw data (the Totals are greater than the sum of the entries (Actual Total)), and in Quarter 4, there were additional entries in the raw data not included in the Total (Actual Total is greater than the Total):

• Q1 April-Jun 2015	Total	391
	Actual Total	391
• Q2 July-Sept 2015	Total	559
	Actual Total	512
• Q3 Oct-Dec 2015	Total	497
	Actual Total	482
• Q4 Jan-Mar 2016	Total	448
	Actual Total	472

The figures used for the purposes of the following pie chart are the Actual Totals using the new groupings details above and show a different picture to the breakdown of Q4 Jan-Mar 2016 than that of the ICO website, above:



Adapted from raw data provided on ICO Website (Aug 2016)

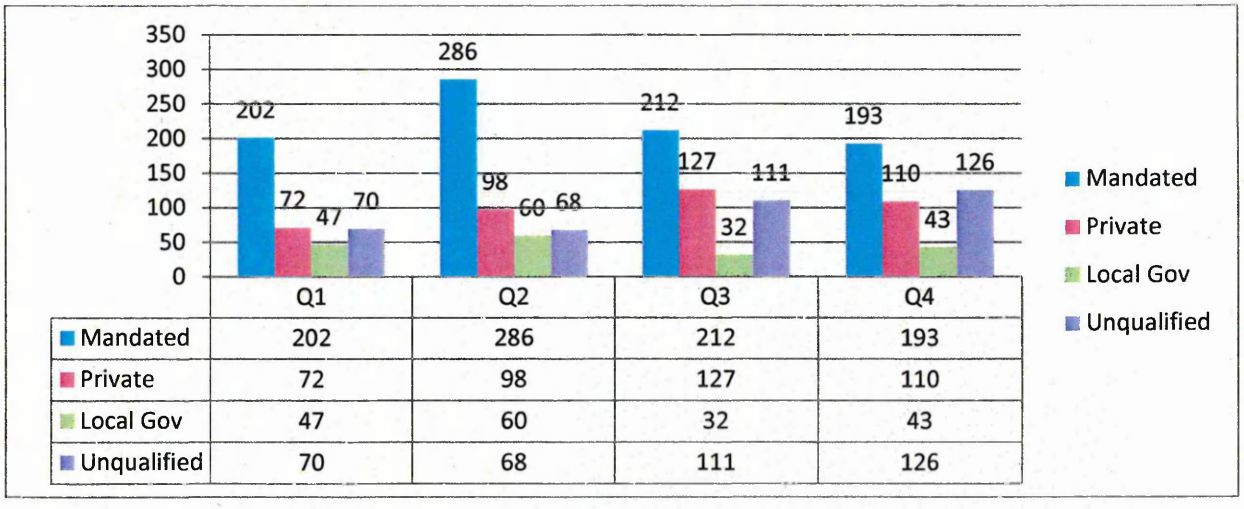


Adapted from raw data provided on ICO Website (Aug 2016)

Instead of local government being the second largest sector reporting breaches incidents from this sector amount to less than 10% of those reported overall. Incidents from those sectors mandated to report breaches to the ICO make up over 40% of the total. This means at least half of the reported cases come from the public sector.

Whilst this does not indicate a good data protection regime within the public sector it is misleading to make any judgements based on this data alone as the figures are not comparing a like for like situation. The data is comparing sectors that must report any breaches to those who are likely to only report breaches if there is a significant risk that the data will be compromised or the breach is already public knowledge. There are also a considerably greater number of private organisations than there are in the public sector; the figures do not indicate the number of breaches reported as a proportion of the sector as a whole. It will be useful to revisit and monitor these data sets once breach reporting becomes mandatory.

The following bar chart compares data within the various sectors over the four quarters to analyse the reporting over time within similar sectors however, there does not appear to be a noticeable trend during the year. Although there are no clear trends to be observed in this breakdown, it is very evident that those sectors mandated to report are doing so significantly more frequently than those with no binding obligation to do so. However, once again no inference can be drawn from this without further details.



	Q1	Q2	Q3	Q4
Mandated	202	286	212	193
Private	72	98	127	110
Local Gov	47	60	32	43
Unqualified	70	68	111	126

Adapted from raw data provided on ICO Website (Aug 2016)

Drilling down into the data on the types of breaches shows that the key reasons for breaches are: the loss or theft of paperwork or unencrypted device; data posted, faxed or

emailed to the wrong person; and insecure webpage or hacking. Once again, there is no discernible trend from the data. It would be a useful exercise to assess the data across a longer period of time and drilling into the detail to ensure that there is a reliable data set to compare results.

A further study by the ICO focuses solely on 16 LAs where it conducted audits during 2013 showed some rather worrying results and a very mixed picture. The LAs were measured over 6 categories: data protection governance; records management; SARs procedure; security of personal data; training and awareness; and data sharing. Of the 16 LAs audited none offered a high level of assurance, only 9 of them had reasonable safeguards in place and the rest had limited or very limited assurance of data protection.

According to a 2015 survey by Big Brother Watch there have been over 4,000 data breaches in LAs in 3 years between 2011 and 2014. The report calls for tougher sanctions for breaches, particularly for those that are deliberate or should have been easy to avoid. From data gathered using Freedom of Information requests they found that "despite more than 400 instances of loss or theft, including 197 mobile phones, computers, tablets and USBs and 600 cases where information was inappropriately shared, just a single person has faced criminal sanctions and only 50 have been dismissed." If the previous predictions regarding the trend towards digitised services is to be believed, the situation regarding data protection will need to improve significantly and having more stringent penalties on individuals than fines for the organisations, which tend to punish the victim of the data breach further by reducing the quality of services they receive, may well by an effective way to achieve this.

Big Brother Watch make the following recommendations:

1. The introduction of custodial sentences for serious data breaches.
2. Where a serious breach is uncovered the individual should be given a criminal record.
3. Data protection training should be mandatory for members of staff with access to personal information.
4. The mandatory reporting of a breach that concerns a member of the public.
5. Standardised reporting systems and approaches to handling a breach.
6. The extension of the ICO's assessment notice powers to cover local authorities.

The report states the limitations on penalties imposed by Section 55 of the DPA, of a maximum fine of £500,000, as the reason why there is more of a trend towards imposing fines on the organisation rather than punishing the individual. It calls for the enactment of the already agreed change to Section 77 of the Criminal Justice and Immigration Act 2008, which will allow custodial sentences of up to 2 years to be imposed on serious or serial offenders, citing the derisory fines imposed on private investigators who hacked mobile phones to obtain information for newspapers as an example of the ineffectual penalties currently in place.

Big Brother Watch sent Freedom of Information requests to all local authorities and report receiving a 98% response rate. Of those who responded, 167 (38%) LAs reported that they had not had any data breaches during the 3-year period requested by Big Brother Watch. This is an extremely interesting insight into the procedures within some LAs. At first glance it would seem that some LAs had a perfect data protection governance structure within the organisation and no mistakes, thefts or incidents of unauthorised access have ever taken place. However, when compared to similar size LAs over the same period of time a more realistic picture of the number of mistakes being made emerges. It is therefore much more likely that the fact that no data breaches are being reporting in these LAs should not necessarily be read as no data breaches having taken place. Whilst it is not possible to prove without undertaking audits of those organisations and some primary research, including observation, it is more plausible to conclude that these organisations either:

a) have varying views on what constitutes a breach and are only reporting the most serious of breaches, which they have not yet experienced;
b) don't keep sufficient records to respond accurately to the FOI request but stated they didn't experience any breaches; or
c) didn't disclose them in the FOI request because they hadn't been reported to the ICO and feared alerting the ICO to this fact or feared damaging their reputation with the general public.

If these 160+ organisations are being truthful and have had no data breaches they would be in a very good position to share best practice with those that reported having a significant number of breaches. Big Brother Watch point out that the lack of a consistent

approach to breach management, punishments and corrective action is a problem. In particular it may be distorting the view of those organisations reporting a high number of breaches who may well be following the correct protocol and taking the responsibility of safeguarding citizens' data seriously. This seems to be borne out by a previous study "Local Authority Data Loss" by Big Brother Watch conducted in 2011, which states that in a study of 100 LAs there were over 1,000 data breaches but only 55 of those were actually reported to the ICO.

The 2015 research cites one example of a high level of reporting at Glasgow City Council. The Council was fine £150,000 after two unencrypted laptops holding over 20,000 council tenant records including their bank details. It went on to explain that Glasgow accounted for 75% of all the equipment thefts reported. This would suggest there is either a great systematic problem in Glasgow or other LAs are under-reporting by comparison. The likely explanation probably lies somewhere between the two.

9.2. Breaches Incurring Monetary Penalties

Whilst the majority of breaches lead to demands for corrective action a number incur significant fines. As well as the more common sanctions of enforcement notices and issuance of undertakings, since 2010 the ICO has issued in excess of £7million in fines, with almost £6million of these going to the public sector. A number of the more serious breaches earning large monetary penalties are outlined below.

Brighton and Sussex University Hospitals NHS Trust

The Financial Services Authority (FSA) works alongside the ICO to regulate organisations working in the financial sector and has considerably more powers to fine organisations for breaches of its regulations than the ICO. The highest fine the FSA has issued so far was £980,000 to Nationwide Building Society over a stolen unencrypted laptop containing the personal details of 11 million customers. In contrast, in the UK currently the maximum fine that can be imposed on an organisation under the Data Protection Act by the ICO is £500,000. The highest fine that has been imposed to date is £350,000, issued to Brighton and Sussex University Hospitals NHS Trust in 2010

Ministry of Justice

In 2014 the Ministry of Justice was fined £180,000 for losing an unencrypted portable hard drive containing details of 16,000 prisoners. It was the second time this type of breach had occurred at the organisation, that time the drive had 3,000 records on it.

Kent Police

In 2012 a policeman, responding to an attempted break-in at premises that had once been a police station, found a box of videotapes of suspect interviews, including some of a convicted child sex offender, left behind by Kent Police when they vacated the building. The new occupier said he had not watched them but had intended to. Kent Police received a fine of £100,000.

Department of Justice Northern Ireland

In 2012 the Northern Ireland Justice Department sold a locked filing cabinet in an auction. When the buyer forced open the lock he found files containing personal details relating to suspected terrorist activities. The new owner reported the find and after taking into account the fact that the cabinet was initially locked, so should have alerted the Data Controller to the fact that there was likely to be something of a sensitive nature in it, it was still sent to auction without any attempt to force it open to find out what its contents were. This lack of action cost the Department of Justice £185,000.

North East Lincolnshire Council

The North East Lincolnshire Council was fined £80,000 in 2011 after a teacher lost an encrypted USB device containing the personal details including dates of birth and physical and mental health reports.

Ministry of Justice

Emails containing sensitive personal information of 1,182 prisoners, including offence information, location within the prison and distinguishing physical features were sent to members of the public, resulting in a £140,000 fine in 2011.

Aberdeen City Council

Four documents containing names, addresses, alleged criminal offences and social care information of children were accidentally uploaded to a public website via an automatic upload programme by an employee working remotely from home in 2012. Despite the information being removed after 4 hours the breach incurred a fine of £100,000 as the ICO deemed that even though the Council was aware there was a risk of a breach from home workers, as evidenced by its Acceptable Use Policy, it had failed to provide adequate equipment to workers to make the home a safe place to work in.

Islington Borough Council

Islington Borough Council were fined £70,000 in 2012 when they responded to 3 separate Freedom of Information Requests made via the website Whatdotheyknow.com, which automatically uploads the responses thereby making them publically available, by attaching a pivot table a summary of data in a spreadsheet. However, the raw data was still included in the spreadsheet in hidden workbooks. The workbooks included 2,375 records including the personal details of housing applicants, including their ethnicity, gender, sexuality, criminal offences and domestic violence.

Powys Council

In February 2011 Powys Council was fined £130,000 for sending details of a child protection case to the wrong recipient. At the time this was the largest fine handed out by the ICO. The Commissioner also warned that a failure to improve staff training would result in court action being taken.

Chief Constable of Dyfed-Powys Police

Chief Constable of Dyfed-Powys Police was fined £150,000 after an email was sent to a member of the public in 2015 containing the personal details of 8 convicted sex offenders.

Chelsea and Westminster Hospital NHS Foundation Trust

After revealing the personal details of over 700 users of an HIV service via email, the Hospital Trust was fined £180,000.

9.3. ICO Audits

Powers have been extended to the new Supervisory Authority (SA) with the Regulation to conduct audits within any organisation in the public or private sector without having to have prior consent or obtaining a court order. This should have a significant impact on the desire for organisations to have the correct compliance regime in place for when the law comes into force.

As has already been stated, accountability is a key theme of the new Regulation and the burden of proof of compliance rests with the organisation; simply stating something is true without being able to prove it by producing documentation may not be enough of a mitigating factor to avoid a penalty in the event of non-compliance or a breach. It is therefore imperative that an organisation has an effective data protection programme that can be backed up by the appropriate documentation.

If an organisation wishes to verify that the measures it has in place will be adequate once the Regulation comes into force it is possible to request an assessment from the ICO who will review policies and procedures in place and suggest any necessary changes.

It is a useful exercise to conduct regular compliance audits within the organisation once the new regime is in place and rectify any issues that are highlighted. This should include spot checks on high risk areas of the business, bogus social engineering attempts to test employees procedures, penetration testing of any IT systems and websites, and such like. Evidence should be kept of the outcomes of the audits to provide to the SA in the event of a breach or an audit.

9.4. Recommended Changes

In order to ensure compliance with the forthcoming legislation it will be necessary for all LAs to review their data protection compliance and assess which policies and procedures may need producing or amending.

It is therefore recommended that a gap analysis be undertaken to consider the changes that may be needed in the areas of the organisation discussed in the following sections. This consists of identifying the required changes to ensure continued compliance once the new legislation is activated and comparing this to current practice within the organisation, then identifying measures to take to bridge the gaps.

9.4.1. Records Management

Notification of data processing activities will no longer be required for most organisations. Only those organisations who have identified that the processing could pose a significant risk to data subjects in the event of a breach are required to register their processing activities with the SA.

Instead of having to notify, organisations will be expected to keep sufficient records to prove compliance with the Regulation, appropriate to the level of risk that is involved with the processing of personal data. This is to ensure that the requirement to keep documentation does not become burdensome for SMEs. It is expected however,

particularly as has been previously stated the majority of the personal data being processed by an LA is likely to fall into the "special category" that all LAs will need to keep detailed records of the measures they take to ensure compliance throughout the organisation.

This is likely to include but is not limited to:

- the upkeep of entries in the organisations risk register;
- a detailed record of Subject Access Requests and any Freedom of Information Requests that required redactions due to the inclusion of personal data;
- a breach management log including any action taken;
- an employee training schedule including dates of sessions completed by individuals;
- an asset register for any digital assets disposed of, including certificates of destruction;
- copies of data protection impact assessments;
- details of Data Protection Officer and Data Owners;
- information flows of the organisation;
- details of all third party organisations who the organisation shares data with;
- a copy of the Information Notice given to data subjects;
- a copy of IT User Policy agreed to by employees; and
- any other policies relating to data security, retention, destruction, storage and portability,

9.4.2. Appointment of a Data Protection Officer

The new Regulation calls for all public sector bodies to appoint a Data Protection Officer (DPO) (or similar title such as Information Governance Officer) to be responsible for ensuring compliance with the Regulation. The DPO must report to the executive committee and have full independence, authority and the resources to carry out the tasks necessary to:

- implement measures to safeguard personal data in business processes and systems development;
- maintain accurate and up to date compliance records;
- undertake a comprehensive training programme throughout the organisation;
- manage personal data access requests (SARs); and
- introduce breach management procedures.

This can be a shared role with another LA or can be a role that is fulfilled by an outsourced organisation. However, given the significant increase in the level of fines that the new Supervisory Authority (SA) will be able to issue for any breach, it is recommended that in larger LAs this be carried out by a dedicated employee of the LA. The DPO should be able to demonstrate a competent level of expertise in the Regulation and be provided with all the resources necessary to ensure that he/she is able to maintain that level of understanding.

Data Owners

To facilitate the role of the DPO and increase the level of responsibility for data protection within the LA it is recommended that each set of personal data that are processed be appointed a Data Owner. This is someone who is responsible for liaising with the DPO on any issues that may arise involving this set of data. Examples of accountability would be to report any data breaches of the data set, make the DPO aware of any changes to the processing activities, and attend meetings during any proposed changes to business processes or systems involved in processing the data.

9.4.3. Undertake a Data Protection Impact Assessment

The first task for the DPO should be to undertake a risk assessment across the organisation in regards to data protection in order to determine where non-compliance issues are more likely to arise.

Conduct a Data Audit

The expansion in the types of data that will be categorised at personal data (IP addresses, location data, pseudonymised data, etc.,) and "special category" data will require a review of the types of data that exist within the organisation. As an extension to the existing data classification system in use in the public sector it is recommended that data types identified are given a further classification of "special category", "personal", with everything else remaining "unclassified". This classification system should be built into any new or reengineered IT systems as discussed further in Section 9.4.4

Once the types of data have been identified and classified it should be possible to identify what processing activities are carried out on the data and how, who accesses the data, where are the data stored, when are they deleted and how.

If none exist already then a useful exercise is to develop information flow (also known as business process flow) models for all those processes that involve personal data identified during the data audit. These diagrams focus on the steps taken during the processing of the data are useful to visualise where the risks may occur. They are also useful tools in training employees new to a role, or for data protection purposes to set a context for the reasons why some steps are required to secure data.

As a useful additional benefit to helping with a data protection impact assessment, information flow diagrams can also help to improve the efficiency of business processes by making it easier to identify where there may be redundant steps within a process.

9.4.4. Introduce Privacy by Design and by Default Development

As part of the move towards greater accountability of actions, all organisations will need to show evidence that any new systems that are developed or existing systems that are to be amended are done so with privacy in mind. This is also the case when designing or reengineering business processes. If there is a way of building data privacy into a system or process, then that must be considered and any rejection of the design must be fully justified. In order to mitigate against a breach that occurs by using a new system or process that could have had greater privacy features included but didn't, it will be down to the organisation to prove that the steps that would needed to be taken would have been too onerous for the organisation to take. Therefore all proof that all possibilities were considered will need to be kept from the discussions on these points.
An example of privacy by default would be to ensure that any portable devices provided by the organisation are encrypted from the outset rather than relying on individual employees to encrypt the device afterwards. Another example would be for the implementation of a robust network password procedure that forces all employees to changes passwords regularly, and to use stronger passwords by not allowing ones that are easy to hack to be accepted. Wherever possible the data subject should be allowed to amend their own details or as a minimum, easily report any errors in the details held to ensure that all information is kept as up to data and accurate as possible.

A more complex example of privacy by design and default would be to introduce the data classification system into IT systems so that it recognises data being processed and restricts certain actions to be undertaken. Another example requiring greater skill and

resources for the IT Department would be to implement pseudonymisation of data sets so that only those individuals that really needed to have the personal details of individuals would have access to them, without restricting access to other details.

9.4.5. Implement a Compulsory and Continuous Training Programme

In order to ensure that all members of staff that handle personal data, or are likely to come into contact with members of the public and therefore at risk of falling victim to social engineering tactics, are aware of their responsibilities regarding the Regulation it is essential that a comprehensive training programme be put in place.

Much like the requirement imposed by health and safety at work laws, this should be compulsory for all members of staff to undertake and should be repeated regularly, particularly, but not confined to, when there are changes in compliance requirements. A record should be kept of all training undertaken and a copy of the proof kept in the employee's training file. Special sessions should be implemented when there is a significant change to legislation, as with the enactment of the Regulation.

Rather than all employees completing the same course, wherever possible training should be tailored to the role the employee undertakes in the organisation and focus on the specific risks entailed in the processing that role involves.

During a presentation on Breach Management at the 2016 ICO Data Protection Practitioners' Conference, Deirdre Allison, (Corporate Records Manager) and Gillian Acheson (Senior Manager Data Protection) from the Belfast Health and Social Care Trust, Northern Ireland, recommended that more innovative approaches to training are taken than the standard "one day spent in a classroom" training session, seen as dry and boring by most attendees.

In 2012 the Belfast Health and Social Care Trust were fined £225,000 for failing to remove sensitive personal data from a decommissioned hospital building. The building was broken into and thieves stole some of the records, which included thousands of patients' medical records as well as 15,000 unopened pay slips of employees, and posted the information on the Internet. After receiving one of the largest fines issued by the ICO the Trust decided to review their entire data protection management.

As part of avoiding what they call the "Seven Deadly Sins of Information Governance" they have introduced data protection into the daily routine of all employees by using innovative methods. Some of these included creating posters, producing silent movies starring staff members, and awarding gold stars to employees demonstrating best practice or showing outstanding vigilance. They stated that the change in the approach to training has also produced a sea-change in the awareness of data protection compliance within the Trust.

Data Protection Champions

One way of ensuring continuity and involvement from members of staff is to appoint Data Protection Champions throughout the organisation who can act as advisors to other staff members, ensure good practice throughout business areas and act as an early warning system for any non-compliance.

9.4.6. Review Third Party Contracts and Data Sharing

It will be necessary to review all contracts with third parties to ensure that shared responsibilities for data protection are adequately reflected in the agreement, now that Data Processors will be bound by the Regulation. It will still be necessary to reiterate what is expected of third parties in the contract so it is still very important that suitably robust clauses are included. It is likely that rather than amending what is currently in place, these will need to be renegotiated and new contracts produced. Having these reviewed by legal experts is likely to be costly but is a necessary overhead in the event that responsibilities are not apportioned appropriately.

Ensure that procedures are put in place to report any data breaches in a timely manner and that in the event these procedures are not upheld by the third party they will be contractually liable for any fines that may be issued as a result. It will also be necessary to do due diligence on the contract and provide proof that this has been undertaken.

Pseudonymisation of data does not discharge the Data Controller from all of its data protection obligations, it is advisable that personal details are removed wherever possible when data is shared or transfer to a third party. Ensure that data is encrypted during the transfer if it is done by means of a portable device or via email for example. If data is accessed via a network, ensure that the security procedures on the network are adequate and that only those with the need to use the data have access to it.

The increased use of cloud service providers requires particular consideration for LAs. It is important that as well as having sound contracts in place, the LA should also be made aware of the location of where processing activities are to take place. For example, if the third party is providing cloud storage, the LA will need to be aware of which countries the servers used by the storage provide are situated. Regardless of whether the cloud provider is established in the EU, if any of the processing activity takes place in a country that is not in the EEA or on the Adequate Countries list (see Section 6.1.8) the safety of the data will need to be reviewed. It can only be transferred to a US company if that company is on a signatory of the EU-US Privacy Shield agreement.

9.4.7. Review Data Storage Policy and Procedures

It is necessary to put adequate safety measures in place for storage of data. If data is stored on the premises of the LA then it is important that any back-up copies of data are kept off premises in a safe and secure location to ensure continuity of business in the event the premises are no longer accessible for whatever reason. These measures should be included in the Contingency Plan that the LA should have in place in the event of a business disaster.

Again, regardless of whether the server is a dedicated one or shared services, any cloud storage should only be used if the server is located in a "safe" country or via an approved US company.

9.4.8. Review Data Retention and Destruction Procedures

Data should only be kept for as long as it is required or for as long as consent is given for it to be processed. It must be disposed of safely and securely. The failure to dispose of data safely is one of the major reasons that organisations have received enforcement notices under the DPA so it is likely that failure to put adequate measures in place, and prove they have been followed correctly, will lead to similar if not more stringent punishment under the Regulation.

It is recommended that the LA implement an Asset Disposal Policy if it does not already have one. This would consist of a set of procedures to safely dispose of any paper files, computers, mobile phones, USB memory sticks, CDs and other portable storage devices. Disposal of paper files may simply involve cross-shredding of personal data. It may

require the services of a confidential waste management organisation to dispose of larger amounts of special category data.

In order for data to be permanently deleted from a hard drive it needs to be wiped forensically. It is therefore necessary to engage the services of a specialist service that will provide a certificate of destruction as proof that each hard drive has been disposed of securely.

9.4.9. Review Employee Handbook and IT User Policy

It is possible to reinforce some measures that can improve the data protection compliance practice throughout the organisation by introducing them in the employee handbook and IT User Policy. If there are no guidelines already for the use of employees' own devices for work purposes then it is important to set some and ensure these are being adhered to. One measure could be the use of partitioning of smart phones and remote locate and wipe software for lost or stolen devices, or the prohibition of the use of unencrypted devices. It is recommended that the LA enforce a clean desk policy on employees dealing in personal data and reiterate the rules regarding unauthorised disclosure of information to third parties.

9.4.10. Review Consent Procedures

It is no longer the case that LAs can rely on "legitimate purpose" as a reason to process data therefore it is important that the procedures and reasons used for processing are reviewed. It may be necessary to obtain explicit consent from data subjects for some of the processing activities.

9.4.11. Review Rights of Data Subjects

The length of time that can be taken to respond to a SAR has been extended but the right to request a fee for the SAR has been removed. New rights have been introduced for data subjects, such as the right to rectification or erasure of data if it is incorrect or invalid and the right to data being provided in a portable format if request. It is important therefore to ensure that new procedures are put in place to allow for any information, resulting from consent being provided in order to be processed, can be compiled into a machine readable format in the event that this is requested by a data subject.

9.4.12. Amend Information Notice

The Information Notice provided to data subjects needs to be amended to include the details of the Data Protection Officer, rules regarding data retention and any changes to the meaning of personal data related to the processing the LA undertakes.

9.4.13. Data Breach Policy

Perhaps one of the most important measures to put in place, especially considering the evidence uncovered by the Big Brother Watch study that a high number of LAs do not appear to have ever experienced a data breach, a data breach notification procedure.

The procedure should include a list of all the situations that constitute a breach and identify a set of steps to take in the event of that situation occurring. The procedures should leave it in no doubt to the employee who they should contact and by when. This should include a detection procedure and response capabilities of the different members of staff, to ensure that the correct procedures are followed by everyone.

Breaches should only be notified to the SA if there is a risk that personal data will be disclosed. If the SA has been notified of a breach and the data in question was not encrypted then it is also necessary to inform the data subject of the breach. Under Article 83(7) the Regulation stipulates the possibility that each member state can enact special rules on breach management and reporting for public sector organisations. It is also down to each member state to determine the sanctions and penalties that each type of data breach is likely to incur. It will be important for each LA to be aware of the specific rules for the UK and ensure it adheres to those rules as well as complying with the Regulation.

In LAs where the processing of personal data is seen as high risk it may be prudent to consider purchasing special insurance to guard against a risk occurring.

10. Conclusion

Data protection has come a long way since the signing of the Universal Declaration of Human Rights in 1948. In 1950 the Council of Europe introduced the Convention for the Protection of Human Rights and Fundamental Freedoms in a bid to cement these rights into the political union formed in Europe after the end of WWII. However, it wasn't until 1981, after several countries had introduced national laws to protect personal data from unchecked interference and undue surveillance from governments and businesses, that the Council of Europe produced a new agreement that made specific reference to an individual's right to the protection of his/her personal data.

Better known as Convention 108, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data formed the basis for European data protection law. As well as providing the early definition of what comprised "personal data", it also set out the principles to be adhered to that are still recognisable in the key piece of EU legislation in force today Directive 95/46/EC, or the Data Protection Directive.

The European Union, in the numerous forms it has taken from the early days of the European Coal and Steel Community in 1951 to the ratification of the Treaty of Lisbon in 2009, has grown from a commercial agreement between 6 countries to an economic and political giant comprising 28 member states, 19 of which share a common currency. This transformation over time has seen powers to propose and enact laws passed to the EU. There are two key types of legislative instruments used by the EU, Directives and Regulations. The current data protection law has been introduced by way of a Directive that sets legal objectives that all EU member states must meet by introducing laws at national level. The national law produced in the UK to enact the Data Protection Directive is the Data Protection Act 1998.

Whilst a Directive allows for some harmonisation of outcomes it still leaves room for interpretation and means to achieve the outcomes to the member states. This can lead to variations throughout the EU countries in implementation and sanctions imposed for non-compliance. This has been the case for data protection legislation, with some countries, such as Germany and Spain, imposing significant sanctions on companies that fail to comply with the law and others, and countries such as the UK being seen by many as having the weakest, most industry-friendly legislation in the EU. It is widely known

that the UK has been the strongest opponent to reforming the current EU data protection laws.

The other legal instrument at the disposal of the EU is a Regulation, which, once agreed, becomes legislation in all member states without the need for member states to create their own laws. This is the most effective way of attaining standardisation of laws throughout the EU. Each member state must adhere to a Regulation and has two years to make the transition. This is the approach that the EU has decided to take with the new data protection legislation. The law comprises a Regulation (*(EU) 2016/679,)* aimed at organisations operating within the internal market and the public sector, and a Directive (*(EU) 2016/680)* to facilitate cooperation between member states on policing and criminal justice matters. The UK, who negotiated a discretionary ability to "opt-out" of certain types of legislation when they signed the Maastricht Treaty, decided to use this privilege when it signed the Lisbon Treaty and opted out of passing powers to legislate over matters of policing and criminal justice to the EU and, as such, will not be bound to introduce laws to enact the Directive. There is also a third directive regarding the sharing of Passenger Name Records ((EU) 2016/681) that as yet it is unclear whether this Directive will be adopted and if so, in what form.

The controversial, and for the most part unexpected, decision by a majority of the UK population to vote in a referendum, held in June 2016, to withdraw from the EU has placed doubt over the legal situation in the UK. It is not yet clear which EU Regulations are likely to be adopted by the UK Parliament once the negotiations to withdraw have been completed and the UK is no longer a member of the EU. Several options are open to the UK, one being the introduction of a piece of legislation in UK law that formally enacts all existing EU legislation. Another, more likely, approach is that all legislation will be assessed individually and some will be revised will others will be adopted in their entirety. Given the level of instability that the UK's decision has brought to the EU, it is unlikely that there will be any appetite within the EU to negotiate a US-style "Privacy Shield" agreement with the UK therefore it is widely recognised that the UK will need to adopt the new data protection Regulation or something very similar if it wishes to sell goods and services to customers in EU countries; this will probably be one of the prerequisites to negotiations given the perception that the Data Protection Act is one of the weakest data protection laws in the EU. It can safely be assumed then that a similar

piece of legislation to Regulation (EU) 2016/679 will be implemented at some point in the near future.

With this in mind, there are a number of changes that will need to be made to the way that organisations safeguard personal data. A key change is to the approach to data protection and a move away from educating organisations after the event towards one of accountability and risk assessment, to proving measures were in place to mitigate against breaches occurring. Reporting of breaches that involve a high risk to the data subjects involved will become mandatory and for any breach where the offending organisation cannot prove they had adequate measures in place to minimise the risk of it occurring, the fine that can be imposed is significantly higher. It will no longer be necessary to register processing activities as a Data Controller with the Supervisory Authority (SA), unless the processing involves a high risk to data subjects. However, the SA will now be able to audit a company without prior consent and a Data Controller must be able to prove compliance by keeping appropriate records or risk sanctions.

Other changes that will be required are the necessity to acquire unambiguous consent of data subjects for some existing processing activities, and the requirement to adopt a "data privacy by design and by default" approach to the development of business processes and systems.

Another key change will be the introduction of a "One Stop Shop" for dealing with organisations established or operating across borders. A new EU institution will be created to deal with complaints from data subjects, harmonisation of sanctions and the standardisation of the implementation of the legislation across member states. Exactly how the UK will interact with the newly created European Data Protection Board has to be determined and will likely be decided as part of the negotiations to withdraw from the EU.

Irrespective of the outcomes of the negotiations, there will likely be a period of overlap during which the new Regulation will come into force and the UK will still be a member of the EU. It is therefore in the interests of all UK organisations, the public sector included, that the next two years is spent preparing for what will be quite a significant overhaul of data protection policies and procedures.

Baroness Neville-Rolfe (2016). The EU Data Protection Package: the UK Government's perspective. [online]. Last updated 2016. https://www.gov.uk/government/speeches/the-eu-data-protection-package-the-uk-governments-perspective.

Big Brother Watch (2011). Local Authority Data Loss November 2011 ed., London, England, Big Brother Watch.

Big Brother Watch (2014). A Breach of Trust. August 2015 ed., London, England, Big Brother Watch.

Cabinet Office (2013). Government Security Classifications. London, England, UK Government.

Cabinet Office (2013). Introducing the Government Security Classifications Core briefing for 3rd Party Suppliers.

CAREY, Peter,LL.M. (2015). Data protection: a practical guide to UK and EU law. Oxford, Oxford University Press.

CARPENTER, Johnny (2015). Are cloud vendors prepared for the impact of this year's EU data regulations? [online]. Last updated 5 February 2015. http://www.techradar.com/news/internet/policies-protocols/are-cloud-vendors-prepared-for-the-impact-of-this-year-s-eu-data-regulations--1283457.

CASTIGLIONE, Paul (2014). European IT Teams Woefully Underprepared for GDPR. [online]. Last updated 18 November 2014. http://www.ipswitchft.com/blog/european-teams-woefully-underprepared-gdpr/.

Computer Weekly Reporters (2016). Facebook data case raises US national security issues. [online]. Computer weekly, http://www.computerweekly.com/news/450299188/Irish-data-protection-case-raises-US-national-security-issues

CONNELLY, Chris (2008). The US Safe Harbor - Fact or Fiction? Australia, Galexia.

Council of Europe (2016). Details of Treaty No 108. [online]. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

Curia (2016). Method of Citing the Case Law. [online]. Last updated 3/5/2016. http://curia.europa.eu/jcms/jcms/P_126035/en/.

Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market. (2015). [online]. European Union News, http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm.

Information Commissioner's Office (2016). Data Protection Practitioners' Conference: Breach Management Presentation by Belfast Health and Social Care Trust (26:08). [online]. Manchester, England, https://www.youtube.com/watch?v=ZwoF9Gq9Pq4.

DE RUYT, Jean and VOS, Sebastian (2015). The EU data protection regulation after 3 years of negotiation. [online]. Last updated 5 January 2015. http://www.insideprivacy.com/international/european-union/the-eu-data-protection-regulation-after-3-years-of-negotiation/.

Edited By Mike McConville And Wing Hong Chui. (2007). Research Methods for Law. [online]. Edinburgh University Press.

Europa (2010). The non-written sources of European law: supplementary law. [online]. Last updated 20/8/2010. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l14533.

Europa (2010). Sources of European Union Law. [online]. Last updated 18/08/2010. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14534.

Europa (2016). Court of Justice of the European Union (CJEU) - Overview. [online]. Last updated 4/6/2016. https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en#goto_2.

Europa (2016). European Court of Auditors - Overview. [online]. Last updated 2016. https://europa.eu/european-union/about-eu/institutions-bodies/european-court-auditors_en.

Europa (2016). How EU decisions are made. [online]. Last updated 14/8/2016. https://europa.eu/european-union/eu-law/decision-making/procedures_en.

Europa (2016). Legislative Procedures. [online]. Last updated 4/7/2016. http://www.europarl.europa.eu/aboutparliament/en/20150201PVL00004/Legislative-powers.

Europa (2016). Overview on Binding Corporate Rules. [online]. Last updated 10/6/2016. http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.

Europa (2016). Regulations, Directives and Other Acts. [online]. Last updated 14/8/2016. https://europa.eu/european-union/law/legal-acts_en.

European Central Bank (2016). About the European Central Bank. [online]. Last updated 2016. https://www.ecb.europa.eu/ecb/html/index.en.html.

European Commission (2003). Analysis and impact study the on implementation of Directive EC 95/46 in member states. Brussels, Belgium,.

European Commission (2010). Data protection: Commission requests UK to strengthen powers of national data protection authority, as required by EU law. European Commission Press Release, 24 June 2010, .

European Commission (2016). About the European Commission. [online]. Last updated 5/5/2016. http://ec.europa.eu/about/index_en.htm.

EUROPEAN COMMISSION (2016). Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. 2016/C 202/1. Brussels, Belgium, .

European Commission (2016). Guide to EU-US Privacy Shield .

European Council (2016). Presidency of the Council of Europe Union. [online]. Last updated 5/5/2016. http://www.consilium.europa.eu/en/council-eu/presidency-council-eu/.

European Data Protection Supervisor (2016). Data protection legislation. [online]. Last updated 2016. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA2.

European Parliament (2016). Civil Liberties, Justice and Home Affairs Committee. [online]. Last updated 6/1/2016. http://www.europarl.europa.eu/committees/en/libe/home.html.

European Parliament (2016). Principles of Subsidiarity (Article 5(3) of the Treaty on European Union (TEU) and Protocol (No 2) on the application of the principles of subsidiarity and proportionality). Brussels, Belgium, .

FireEye (2015). Mixed state of readiness for new cybersecurity regulations In Europe. IDG Connect.

GILBERT, Francoise (2012). Proposed EU data protection regulation: the good, the bad, and the unknown. [online]. Journal of internet law, 15 (10), .

GILBERT, Françoise (2014). Proposed Eu Data Protection Regulation-Issues To Consider When Planning For The Future Regime. [online]. Journal of internet law, 17 (12), 1.

GPEN (2016). Global Privacy Enforcement Network Annual Privacy Sweep Report 2016. Unknown,.

GRAHAM, Christopher (2016). Referendum result response of Information Commissioner's Office. [online]. Last updated 2016. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/07/referendum-result-response/.

GREEN, Chloe (2014). EU Regulation: time to act on corporate data protection. [online]. Last updated 24 August 2014. http://www.information-age.com/industry/uk-industry/123458394/eu-regulation-time-act-corporate-data-protection.

HARRELL, Corey (2009). Reducing Data Breaches. [online]. Edpacs, 39 (1), 10-15.
Hunton & Williams (2016). EU Data Protection Regulation Tracker. [online]. Last updated 2016. https://www.huntonregulationtracker.com/legislativescrutiny/.

Information Commissioner's Office (2012). Model Contract Clauses International Transfers of Personal Data. [online]. Last updated 28/02/2012. https://ico.org.uk/media/1571/model_contract_clauses_international_transfers_of_personal_data.pdf.

Information Commissioner's Office (2013). Data Protection Regulatory Action Policy. [online]. Last updated 07/18/2013. https://ico.org.uk/media/about-the-ico/policies-and-procedures/1853/data-protection-regulatory-action-policy.pdf.

Information Commissioner's Office (2014). Findings from ICO audits of 16 local authorities. Manchester, England, Information Commissioner's Office. (January to December 2013).

Information Commissioner's Office (2014). Findings from ICO audits of 16 local authorities: January to December 2013. London, UK, Information Commissioner's Office.

Information Commissioner's Office (2014). Local authorities audit report: "areas of good practice, but clear room for improvement by all". ICO News, 26 August 2014, .

Information Commissioner's Office (2015). Taking action - data protection. [online]. Last updated 2015. https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/.

Information Commissioner's Office (2016). Data Security Incidents. [online]. Last updated 29 April 2016. https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

Information Commissioner's Office (2016). Referendum Result Response. [online]. Last updated 24 June 2016. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/06/referendum-result-response/.

Information Commissioner's Office (Unknown). Local Government. [online]. Last updated Unknown. https://ico.org.uk/for-organisations/local-government/.

International Trade Administration US (2016). EU-US Privacy Shield Framework, Key New Requirements for Participating Companies. [online]. Last updated 2016. https://www.privacyshield.gov/Key-New-Requirements.

KOOPS, Bert-Jaap (2014). The trouble with European data protection law. [online]. International data privacy law, 4 (4), 250.

Law Society (2014). Cloud Computing - Practice Note. [online]. Last updated 7 April 2014. http://www.lawsociety.org.uk/support-services/advice/practice-notes/cloud-computing/.

LLOYD, Ian J. (2014). Information technology law. [online]. Oxford, Oxford University Press.

MCCONVILLE, Michael and CHUI, Wing Hong (2007). Research methods for law. [online]. Edinburgh, Edinburgh University Press.

National Audit Office (2012). A Short Guide to Regulations. London, England, NAO Communications.

National Audit Office (2012). A Short Guide to the NAO's Work on Local Authorities. London, England, NAO Communications.

OECD (2013). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [online]. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

OECD (Unknown). Organisation for Economic Co-operation and Development - What We Do and How. [online]. http://www.oecd.org/about/whatwedoandhow/.

Office for National Statistics London, England,UK labour market: June 2016 .

PALMER, Danny (2014). ICO issues warning to law firms following string of data breaches. Computing, August .

PLIMMER, Gill (2014). UK Outsourcing Spend Doubles to £88bn Under the Coalition. [online]. Last updated 6 July 2014. http://www.ft.com/cms/s/0/c9330150-0364-11e4-9195-00144feab7de.html#axzz4DutWzSjl.

POLCÁK, Radim (2014). Getting European data protection off the ground. [online]. International data privacy law, 4 (4), 282.

Progressive Digital Media (2014). ICO publishes local authorities audit. Progressive Digital Media Technology News, Aug 27, 2014, .

Public Sector Executive (2016). Council spending on outsourcing rises 23% year-on-year Manchester, England, Cognitive Publishing Ltd.

REED, Chris (2011). Computer law. [online]. Oxford, Oxford University Press.

Report: Functions, powers and resources of the Information Commissioner. (2013). UK Regulatory Materials Summaries, 21 March, .

ROSSI, Ben (2015). Countdown to the EU General Data Protection Regulation: 5 steps to prepare. [online]. Last updated 24 March 2015. http://www.information-age.com/it-management/risk-and-compliance/123459219/countdown-eu-general-data-protection-regulation-5-steps-prepare.

Information Commissioner's Office (2015). Simon Hughes speech to ICO's 2015 Data Protection Practitioner Conference. [online]. London, Information Commissioner's Office. 2nd March 2015. https://icoconference2015.wordpress.com/speakers/.

SMITH, David (2015). Three years on....and still waiting for reform. ICO News Blog. [online]. Posted 6 February 2015. https://iconewsblog.wordpress.com/2015/02/06/three-years-on-and-still-waiting-for-reform/.

SUGDEN, Martin (2014). Local authorities: Facing up to data loss. [online]. Last updated 23 September 2014. http://www.localgov.co.uk/Local-authorities-facing-up-to-data-loss/37267.

TREACY, Bridget (2013). UK businesses cannot ignore the EU's data protection reforms. [online]. Last updated 7 August 2015. http://www.information-age.com/it-management/risk-and-compliance/123457253/uk-businesses-cannot-ignore-the-eu---s-data-protection-reforms-.

TRIGER, Loic (2014). Changes in European Data Protection Regulation: A look at the GDPR. [online]. Last updated 30 December 2014. http://www.techradar.com/news/internet/policies-protocols/changes-in-european-data-protection-regulation-a-look-at-the-gdpr-1278235/2.

UK Houses of Parliament (2016). Improving government data to transform public services. [online]. Last updated 2016. https://www.gov.uk/government/news/improving-the-way-government-shares-data-to-transform-public-services.

UNITED NATIONS (1948). The Universal Declaration of Human Rights. Paris, France, Bill General Assembly Resolution 217(III) .

VAN HOBOKEN, Joris, ARNBAK, Axel and VAN EIJK, N. A. M. N. (2012). Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act. [online]. Social science research network, November 27 2012 .

WALLIMAN, Nicholas S. R. (2011). Research methods: the basics. [online]. London, Routledge.

WEBSTER, Mandy (2011). Effective data protection: managing information in an era of change. [online]. London, ICSA.

WRIGHT, D. and WADHWA, K. (2013). Introducing a privacy impact assessment policy in the EU member states. [online]. International data privacy law, 3 (1), 13-28.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2010). Opinion 8/2010 on applicable law Adopted on 16 December 2010. 0836-02/10/EN WP 179.

BOT, Yves (2015). Court of Justice of the European Union PRESS RELEASE No 106/15 Luxembourg, 23 September 2015 Advocate General's Opinion in Case C-362/14 Maximillian Schrems v Data Protection Commissioner . Luxembourg.

C-101/01 (judgment of 6 November 2003) / Reference for a preliminary ruling from the Göta hovrätt : Bodil Lindqvist (2003). European Court of Justice.

Case C-131/12: Judgment of the Court (Grand Chamber) of 13 May 2014. Brussels, Belgium.

Case C 230/14, REQUEST for a preliminary ruling under Article 267 TFEU from the Kúria (Hungary), made by decision of 22 April 2014, received at the Court on 12 May 2014, in the proceedings Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság,(2012). European Court of Justice.

Case C 362/14, REQUEST for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), made by decision of 17 July 2014, received at the Court on 25 July 2014, in the proceedings Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd (2014). European Court of Justice.

Central London Community Healthcare NHS Trust v Information Commissioner (2013). UK.

Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters. (2008). OJ L 350 30.12.2008. Brussels, Belgium.

COUNCIL OF EUROPE (1950). Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11. Rome, Italy.

COUNCIL OF EUROPE (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, France.

Durant v Financial Services Authority [2003] EWCA Civ 1746, [2004] FSR 573 CA.

ECLI:EU:C:2014:317 C 131/12, REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Nacional (Spain), made by decision of 27 February 2012, received at the Court on 9 March 2012, in the proceedings Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,(2014). European Court of Justice.

EUROPEAN COMMISSION (1957). Treaty establishing the European Economic Community, EEC Treaty - original text (non-consolidated version). Unpublished 25.3.1957. Rome, Italy.

EUROPEAN COMMISSION (1988). Commission Directive 88/301/EEC of 16 May 1988 on competition in the markets in telecommunications terminal equipment. OJ L 131, 27.5.1988. Brussels, Belgium.

EUROPEAN COMMISSION (1992). Treaty on European Union. OJ C 191, 29.7.1992. Maastricht, Germany.

EUROPEAN COMMISSION (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Official Journal L 281 , 23/11/1995 P. 0031 - 0050. Luxembourg.

EUROPEAN COMMISSION (1997). Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, signed at Amsterdam, 2 October 1997. 97/C 340 /01. Amsterdam, Netherlands.

EUROPEAN COMMISSION (2000). 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441). OJ L 215 25.08.2000.

EUROPEAN COMMISSION (2000). Charter of Fundamental Rights of the European Union. OJ C 364/1 18.12.2000.

EUROPEAN COMMISSION (2001). Treaty of Nice Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts. OJ C 80 10.3.2001.

EUROPEAN COMMISSION (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201/37 31.7.2002. Brussels, Belgium.

EUROPEAN COMMISSION (2006). Commission Directive 2006/111/EC of 16 November 2006 on the transparency of financial relations between Member States and public undertakings as well as on financial transparency within certain undertakings (Codified version) . OJ L 318/17 17.11.2006. Brussels, Belgium.

EUROPEAN COMMISSION (2007). Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community. 12007L/TXT OJ C 306 17.12.2007.

EUROPEAN COMMISSION (2008). Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350 30.12.2008. Brussels, Belgium.

EUROPEAN COMMISSION (2012). Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on European Union - Protocols - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007. OJ C 326, 26.10.2012.

EUROPEAN COMMISSION (2012). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) / COM/2012/011 final - 2012/0011 (COD) */. 52012PC0011. [online]. Brussels, Belgium, http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011.*

EUROPEAN COMMISSION (2012). Rules of Procedure of the Court of Justice of 25 September 2012. OJ L:2012:265 27.09,2012. Luxembourg.

EUROPEAN COMMISSION (2014). Right to be forgotten on the Internet: RULING OF THE EUROPEAN COURT OF JUSTICE

EUROPEAN COMMISSION (2016). Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. C(2016) 4176 final 12.7.2016. Brussels, Belgium.

EUROPEAN COMMISSION (2016). Commission decisions on the adequacy of the protection of personal data in third countries. Brussels, Belgium.

EUROPEAN COMMISSION (2016). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. 32016L0680 OJ L 119/89 4.5.2016. Brussels, Belgium.

EUROPEAN COMMISSION (2016). DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. 32016L0681 OJ L 119/132 27.4.2016. Brussels, Belgium.

EUROPEAN COMMISSION (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 32016R0679 OJ L 119/1 27.04.2016. Brussels, Belgium.

EUROPEAN DATA PROTECTION COMMISSIONERS (2012). Resolution on the European data protection reform. Luxembourg.

Great Britain. Lord Chancellor's Office, Great Britain. Scottish Office and Great Britain. Home Office (1972). Report of the Committee on Privacy. [online]. H.M.S.O. , 5012.

HUSTINX, PETER (2015). Opinion of the European Data Protection Supervisor on the Data Protection Reform Package Brussels, Belgium.

Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner (2015). Court of Justice of the European Union.

UK HOUSES OF PARLIAMENT (1972). European Communities Act 1972. London, England.

UK HOUSES OF PARLIAMENT (1998). Data Protection Act 1998. London, England.

UK HOUSES OF PARLIAMENT (2000). Freedom of Information Act 2000. 2000 c.36. London, England.

UK HOUSES OF PARLIAMENT (2000). Local Government Act 2000. 2000 c.22. London, England.

UK HOUSES OF PARLIAMENT (2003). The Privacy and Electronic Communications (EC Directive) Regulations 2003. 2003 No. 2426. London, England.

UK HOUSES OF PARLIAMENT (2011). Localism Act 2011. 2011 c.20.

UK HOUSES OF PARLIAMENT (2011). The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 2011 No. 1208. London, England.

UK HOUSES OF PARLIAMENT (2014). The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014. 2014 No. 3141. London, England.

UK HOUSES OF PARLIAMENT (2014). Data Retention and Investigatory Powers Act 2014. 2014 c.27. London, England.

UK HOUSES OF PARLIAMENT (2016). Investigatory Powers Bill. HL Bill 40. London, England.

UK HOUSES OF PARLIAMENT (2016). Digital Economy Bill (HC Bill 45). London, UK, UK Parliament, Bill HC Bill 45 2016-17 (2nd Reading House of Commons).

UNITED NATIONS (1984). Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. New York, USA, Bill A/RES/39/46 (39th Session Plenary 93). Central London Community Healthcare NHS Trust v Information Commissioner (2013). UK.

Appendices

1. Data Protection Safe Countries

2. Types of Data Breaches Reported by Sector

Appendix 1 - Data Protection Safe Countries

EU Countries

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

EEA Countries

Iceland
Lichtenstein
Norway

Countries Receiving EU Adequacy Approval

Andorra,
Argentina,
Canada (commercial organisations),
Faeroe Islands,
Guernsey,
Israel,
Isle of Man,
Jersey,
New Zealand,
Switzerland and
Uruguay

Self-certification Adequacy Agreement

United States of America

Appendix 2 - Types of Data Breaches Reported by Sector

Breakdown compiled from raw data set provided by ICO

Breakdown of Types of Data Breaches Reported by Sector (Compiled from ICO raw data set)

Q1 April - June 2015	TOTAL	Central government	Health	MANDATED	Education	Charitable	Justice	Finance, insurance & credit	General business	Retail and manufacture	Utilities	Land or property services	Legal	Marketing	Media	PRIVATE	Members	Online	Political	Regulators	Religious	Social Care	Transport & Leisure	Other	LOCAL GOV	UNQUALIFIED	ACTUAL TOTAL
Loss or theft of paperwork	91	0	64	64	1	3	3	4	2	0	0	0	2	0	0	8	0	0	0	3	0	0	0	0	9	10	91
Data posted or faxed to incorrect recipient	90	3	50	53	0	1	1	10	2	0	1	1	0	0	1	15	0	0	0	3	0	0	0	0	17	5	90
Data sent by email to incorrect recipient	33	2	15	17	1	0	1	0	1	0	0	1	2	0	0	4	1	0	1	0	0	0	0	2	6	6	33
Insecure webpage (including hacking)	21	0	4	4	1	1	0	1	3	1	0	1	0	0	0	6	0	5	0	0	0	0	1	1	2	9	21
Loss or theft of unencrypted device	28	1	7	8	5	2	1	2	2	1	0	2	2	0	0	9	0	0	0	1	0	0	1	0	1	10	28
Insecure disposal of paperwork	10	0	4	4	1	0	0	1	0	0	0	2	0	0	0	3	0	0	0	0	0	1	0	0	1	2	10
Failure to redact data	16	1	8	9	1	0	0	2	1	0	0	0	0	0	0	3	0	0	0	1	0	0	0	0	2	2	16
Information uploaded to webpage	5	1	1	2	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	5
Verbal disclosure	7	0	2	2	2	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	2	2	7
Insecure disposal of hardware	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Other principle 7 failure	89	1	37	38	6	4	7	4	10	1	0	1	4	0	2	22	4	1	0	0	0	0	1	0	6	23	89
Total	**391**			**202**												**72**									**47**	**70**	**391**

Q2 July - September 2015	TOTAL	Central government	Health	MANDATED	Education	Charitable	Justice	Finance, insurance & credit	General business	manufacture	Utilities	Land or property services	Legal	Marketing	Media	PRIVATE	Members	Online	Political	Regulators	Religious	Social Care	Transport & Leisure	Other	LOCAL GOV	UNQUALIFIED	ACTUAL TOTAL
Loss or theft of paperwork	120	3	74	77	1	3	3	4	2	0	0	2	7	0	0	15	0	0	0	3	0	0	0	0	12	10	114
Data posted or faxed to incorrect recipient	100	0	62	62	0	1	1	6	2	0	0	1	8	0	1	18	0	0	0	3	0	0	0	1	9	6	95
Data sent by email to incorrect recipient	85	1	32	33	1	0	1	7	4	3	0	1	1	0	0	16	1	0	1	0	0	0	0	0	10	4	63
Insecure webpage (including hacking)	39	0	5	5	1	1	0	2	3	8	0	3	1	0	0	17	0	5	0	0	0	0	1	0	5	8	35
Loss or theft of unencrypted device	30	0	11	11	5	2	1	2	2	0	0	3	2	0	0	9	0	0	0	1	0	0	1	0	2	10	32
Insecure disposal of paperwork	28	1	18	19	1	0	0	3	0	0	0	2	1	0	0	6	0	0	0	0	0	1	0	0	2	2	29
Failure to redact data	18	2	1	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	8	2	13
Information uploaded to webpage	13	0	3	3	1	0	0	1	1	0	0	0	1	0	0	3	0	0	0	0	0	0	0	0	4	1	11
Verbal disclosure	10	0	7	7	2	0	0	0	0	0	0	1	0	0	1	2	0	0	0	0	0	0	0	0	0	2	11
Insecure disposal of hardware	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other principle 7 failure	116	1	65	66	6	4	7	6	1	1	0	2	0	0	2	12	4	1	0	0	0	0	1	0	8	23	109
Total	**559**			**286**												**98**									**60**	**68**	**512**

Q3 October - December 2015	TOTAL	Central government	Health	MANDATED	Education	Charitable	Justice	Finance, insurance & credit	General business	manufacture	Utilities	Land or property services	Legal	Marketing	Media	PRIVATE	Members	Online	Political	Regulators	Religious	Social Care	Transport & Leisure	Other	LOCAL GOV	UNQUALIFIED	ACTUAL TOTAL
Loss or theft of paperwork	70	4	35	39	3	6	2	3	2	0	0	1	4	0	0	10	0	0	0	1	1	0	0	0	4	13	66
Data posted or faxed to incorrect recipient	83	0	53	53	2	0	6	5	2	0	1	1	2	0	1	12	1	0	0	2	0	0	0	0	10	11	86
Data sent by email to incorrect recipient	88	2	31	33	9	2	5	7	7	1	1	5	3	0	0	24	3	0	1	4	0	0	1	0	5	25	87
Insecure webpage (including hacking)	59	1	2	3	5	2	0	6	19	4	2	1	1	0	0	33	1	2	0	0	0	0	1	0	2	11	49
Loss or theft of unencrypted device	30	0	10	10	2	1	3	4	2	0	0	0	4	0	0	10	1	0	0	0	0	0	1	0	0	8	28
Insecure disposal of paperwork	15	0	7	7	0	0	1	1	1	0	0	1	1	0	0	4	0	0	0	0	0	0	0	0	0	1	12
Failure to redact data	13	0	2	2	4	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	5	7	15
Information uploaded to webpage	10	0	2	2	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	2	3	8
Verbal disclosure	3	0	1	1	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	1	0	1	2	5
Insecure disposal of hardware	2	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Other principle 7 failure	124	1	60	61	16	5	6	13	9	0	0	5	4	0	0	31	0	1	0	1	0	1	0	0	3	30	125
Total	**497**			**212**												**127**									**32**	**111**	**482**

Q4 January - March 2016	TOTAL	Central government	Health	MANDATED	Education	Charitable	Justice	Finance, insurance & credit	General business	manufacture	Utilities	Land or property services	Legal	Marketing	Media	PRIVATE	Members	Online	Political	Regulators	Religious	Social Care	Transport & Leisure	Other	LOCAL GOV	UNQUALIFIED	ACTUAL TOTAL
Loss or theft of paperwork	74	3	36	39	3	8	3	3	4	1	0	3	7	0	2	20	0	0	0	0	0	1	0	0	6	15	80
Data posted or faxed to incorrect recipient	74	1	41	42	3	0	4	5	1	0	0	2	3	0	0	11	0	0	0	0	0	0	1	1	10	9	72
Data sent by email to incorrect recipient	42	0	14	14	11	4	2	3	5	0	0	0	4	0	0	12	2	0	0	2	0	0	4	1	3	26	55
Insecure webpage (including hacking)	39	0	1	1	7	3	0	4	15	3	0	0	0	0	0	22	0	7	0	0	0	0	4	2	2	23	48
Loss or theft of unencrypted device	20	2	1	3	5	2	0	1	1	0	0	0	2	0	0	4	1	1	0	0	0	0	1	0	1	10	18
Insecure disposal of paperwork	24	0	17	17	2	0	2	0	0	0	0	0	2	0	0	2	0	0	0	0	0	0	0	0	1	4	24
Failure to redact data	28	0	10	10	2	0	1	1	0	0	0	4	1	0	0	6	0	0	0	0	0	1	0	0	7	4	27
Information uploaded to webpage	10	0	3	3	4	0	0	1	1	0	0	1	1	0	0	4	0	0	0	1	0	0	0	0	2	5	14
Verbal disclosure	7	0	2	2	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	2	1	6
Insecure disposal of hardware	2	0	1	1	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	3
Other principle 7 failure	128	3	58	61	11	6	4	6	9	0	0	7	5	0	0	27	0	2	1	1	1	0	2	0	9	28	125
Total	**448**			**193**												**110**									**43**	**126**	**472**