Challenges old and new: An analysis of the impacts of the General Data Protection Regulation

Neil Fraser

Technical Report

RHUL–ISG–2018–4

3 April 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

100845888
Neil Fraser

Challenges Old and New: An Analysis of the Impacts of the General Data Protection Regulation

Supervisor: Geraint Price

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

Art.	Article (of EU legislation)
BCR	Binding Corporate Rules
Brexit	UK Withdrawal from the European Union
BYOD	Bring Your Own Device
CCTV	Closed Circuit Television
CISO	Chief Information Security Officer
CJEU	Court of Justice of the European Union
CoE	Council of Europe
COTS	Commercial-off-the-Shelf (referring to products or services)
CSP	Communications Service Provider
DoS	Denial of Service (attack)
DPA	New UK Data Protection Act (replacement for DPA98)
DPA84	Data Protection Act 1984 (UK legislation)
DPA98	Data Protection Act 1998 (UK legislation)
DPD95	Data Protection Directive 1995 (EU legislation)
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DPR	Data Protection Registrar (predecessor of ICO)
EC	European Commission
ECHR	European Convention on Human Rights (CoE treaty)
EDPB	European Data Protection Board (successor of WP29)
EDPS	European Data Protection Supervisor
EEA	European Economic Area (EU plus Iceland, Lichtenstein and Norway)
EU	European Union
GDPR	General Data Protection Regulation (EU legislation)
ICO	Information Commissioner's Office
IoT	Internet of Things
IPA16	Investigatory Powers Act 2016 (UK legislation)
ISMS	Information Security Management System
NHS	National Health Service (UK)
PbD	Privacy by Design
PCI-DSS	Payment Card Industry Data Security Standard
RBAC	Role Based Access Control
Rec.	Recital (of EU legislation)
SA	Supervisory Authority (for data protection)
SAR	Subject Access Request
SME	Small to Medium Enterprise (10 – 249 employees)
WP29	Article 29 Data Protection Working Party (EU advisory body)

EXECUTIVE SUMMARY

The *General Data Protection Regulation* (GDPR) will come into force on 25 May 2018. Its intent is to harmonise data protection laws and provide individuals with increased control over how their personal data is collected and used. By obligating companies to protect and use responsibly the personal data in their care, GDPR seeks to reinforce trust in organisations, support the development of new technologies and boost the digital economy. GDPR brings benefits to business in the form of improved consistency, relaxed notification requirements and clearer guidance on certain aspects of data protection. It also brings certain challenges, however, and the potential for significantly increased monetary penalties in cases of non-compliance.

Certain aspects of GDPR - including, unsurprisingly, the scale of potential penalties - have been subject to much discussion in the academic literature and general media. Others have been overlooked or at least partially misunderstood. Examples of the latter include questions relating to the Regulation's applicability to smaller organisations and how it will affect UK business after the country's withdrawal from the European Union. It is also fair to say that there has been a certain amount of 'scare-mongering' and, in some cases, the Regulation has been presented as being more onerous than it may prove to be. GDPR does bring new challenges to organisations, however, and some are not fully aware or prepared for its introduction. Even for those that are aware, questions remain: exactly what has changed, what does it mean for business, and how can organisations prepare?

Providing answers to these questions is the purpose of this report. It sets out to examine how GDPR differs from previous and current data protection laws and provides a synthesis of the key practical challenges for organisations handling personal data. In critically comparing GDPR with its predecessors, we discover that the underlying principles have remained largely intact since at least the 1970s. While these have been updated to consider new technologies and working practices, the measures to be taken are broadly consistent with the current regime. Only in certain areas does GDPR present markedly new challenges. These include changes to the rules surrounding consent, security of processing, accountability and data subject rights. Even where new challenges do exist, we identify that they are evolutionary and organisations already compliant with existing laws are well placed to deal with and, indeed, benefit from them. In a world where stories concerning cyber-attacks and personal data breaches are becoming common features in the mainstream media, providing good data protection could act as a powerful market differentiator in attracting consumers increasingly aware of the risks.

At its heart, GDPR is about good information governance: knowing what data is held, from whom and for what purpose it was obtained, where it is located and how it is protected. This report argues that, in this regard, GDPR-compliance and, indeed, data protection more generally, shares a great deal in common with the information security function. The two have complementary requirements and measures taken to meet obligations under GDPR have the potential to improve efficiency and the security of business data more generally. The Regulation thus provides an opportunity to drive convergence between data protection and security to benefit organisations while at the same time protecting individual rights.

PART 1: INTRODUCTION AND PROJECT OVERVIEW

1.1 Introduction

The European Union (EU) *General Data Protection Regulation* (GDPR) [1] was adopted on 27 April 2016 and has full legal effect from 25 May 2018. Unlike its predecessor, the *Data Protection Directive 1995* (DPD95) [2], GDPR does not require enabling national legislation; it applies directly and universally across all EU member states. It provides increased rights to individuals and facilitates the free flow of information throughout the EU, while also introducing new challenges for organisations. In the UK, GDPR will replace the *Data Protection Act 1998* (DPA98) [3]. Following a referendum to leave the EU in June 2016 (Brexit), the British government confirmed that GDPR will be adopted [4] and operate as primary legislation until the implementation of a new Data Protection Act (DPA) incorporating the requirements of the Regulation [5].

Technological developments such as social networking, big data, electronic commerce and mobile devices, along with increased computational power and storage capacity, allow organisations to collect and process more personal data than was previously possible. This can benefit individuals and business but it also presents risks to privacy and obligates organisations to protect users' data and maintain their trust [6]. By strengthening individual rights over how data is collected and used, GDPR seeks to reinforce trust in organisations, support development of new technologies and boost the digital economy [7]. For organisations that fail in this regard, GDPR significantly increases the scale of potential penalties for non-compliance. In the UK, the maximum fine increases from £500,000 to €20m (£17m under the proposed DPA) or 4% of global annual turnover for the preceding financial year, whichever is greater.

Over 60% of UK businesses hold personal information on their customers [8], yet only 23% of people trust them to protect it [9]. In 2016, the UK data protection regulator was the second most active in Europe, increasing sanctions 155% over the previous year [10]. GDPR - and its proposed UK counterpart - will be a key consideration for business in the coming years but not only from a compliance perspective: getting data protection right is also an opportunity to build trust and gain a competitive advantage.

1.2 Project Motivation, Aims and Objectives

GDPR will be enforceable immediately from May 2018 and certain aspects of the Regulation will require organisations to proactively adapt working practices currently compliant with DPA98. This will take time but with less than twelve months remaining, many businesses - especially small to medium-sized enterprises[1] (SMEs) - lack awareness or are unsure if they will meet the deadline [11, 12].

[1] As per [8], small (10-49 employees), medium (50-249 employees) and large (250+ employees).

The motivation for this project is the need to better understand a piece of legislation that could disrupt current business practices and which will undoubtedly shape future decision-making. It aims to support GDPR implementation by clarifying how it differs from current requirements and discussing the practical challenges introduced by those changes.

At a high level, the aims of GDPR are not significantly different from those of earlier data protections laws; only the means by which those aims are achieved and the penalties for failure are different. We observe that GDPR is evolutionary, not revolutionary, in nature. This report also argues that data protection should not be viewed as an issue of mere compliance. It can provide mutual benefit to other functions like information security and data governance. Many of the steps needed to comply with GDPR complement those necessary to provide security for business information more generally.

This report is based on the research question: what are the key operational impacts of GDPR for UK organisations handling personal data? This broad aim is further broken down into the following objectives.

- To understand how the motivation and requirements of UK/EU data protection laws have developed over time.
- To define and clarify the scope and key requirements of the GDPR.
- To compare the requirements of existing legislation with the GDPR and highlight key changes.
- To discuss the main challenges presented by GDPR, providing practical advice for how organisations may approach them.

1.3 Methodology

By its nature, this project is exclusively theoretical. Its methodology is based on reviewing relevant academic, legal and regulatory literature, as well researching and evaluating available industry and open source material. It incorporates a broad range of sources from government white papers, journals and conference presentations to articles in the general media. This is deliberate as, although the latter may be considered to lack academic rigour, it is through such material that many organisations affected by GDPR will obtain their knowledge and understanding. It is thus necessary to examine freely available information to highlight areas that have been improperly understood and provide clarification. The topic of this project is also contemporaneous in nature and important guidance continues to be published by relevant authorities. Because there does not yet exist a large corpus of academic discussion on GDPR, we dispense with a discrete background literature review and instead incorporate existing work where relevant. Although this report attempts to capture the most recent opinion and guidance it must, by necessity, be time limited. The cut-off for inclusion of new material is 19 August 2017.

The report is organised as follows. Part 2 presents an overview of the development of European and UK privacy and data protection legislation up to the currently active DPD95/DPA98. This is to demonstrate that common principles have remained at the heart of data protection law since its

inception. Part 3 examines the motivation, scope and requirements of GDPR itself. It seeks to provide clarity on what data is covered and issues such as SMEs and the question of Brexit. Part 4 provides a comparison with existing legislation to identify key changes. Part 5 examines in more detail several aspects of GDPR judged to present the greatest challenge including consent, accountability, security and data subject rights. Part 6 concludes the report.

1.4 A Note on Terminology

This report relies heavily on the text of GDPR. It is thus necessary to introduce the reader to two terms used in European legislation: article (Art.) and recital (Rec.). The articles set out the 'rules' that must be followed; it is failure to comply with a particular article that could result in penalty. The recitals offer greater detail and guidance on how an article should be applied. A court or other authority will often consider the recitals in determining whether the Regulation has been breached. The reader should assume all in-text citations of articles or recitals - e.g. [Art.1(1a)] - refer to GDPR unless otherwise specified.

PART 2: ORIGIN AND EVOLUTION OF DATA PROTECTION

2.1 Introduction

Although this report is primarily concerned with contemporary developments, it is important to recognise GDPR's similarities with past legislation. This section discusses the evolution of European and UK data protection rules up to and including DPD95/DPA98. It is anticipated that the reader will recognise common themes and principles that have remained extant throughout.

2.2 Europe's First Steps

The first legal protections for personal information originated in the aftermath of the Second World War. Following the rise to power of the Nazi Party in 1930s Germany, the government began collecting information on individuals deemed to represent a threat to the state [13]. Based on national census data and tabulated on punch cards, it included racial and ethnic origin, political affiliation, trade-union membership, health and sexual data and religious beliefs [14, 15]. Readers familiar with contemporary data protection laws will recognise these as the special categories of sensitive personal data to which additional protections apply. Indeed, it is for precisely this reason these types of data are considered sensitive. Ultimately, the records would become the basis for a national register of undesirable elements, facilitating the arrest, deportation and murder of millions of citizens [16, 17, 18].

The realisation that personal information could be so misused lead directly to the earliest privacy protections [19, 20]. In 1948, Art.12 of the *Universal Declaration of Human Rights* [21] became the first global expression of a fundamental right to privacy. In Europe, this was formally recognised in 1950 when the newly formed Council of Europe (CoE) drafted the *Convention for the Protection of Human Rights and Fundamental Freedoms* [22], more commonly called the European Convention on Human Rights (ECHR). Art.8 of this treaty affords legal protection from interference by public authorities in one's private and family life.

As an aside, the CoE should not be confused with the EU. The two are discrete organisations with different memberships and legislative bodies, although all members of the EU must also be members of the CoE. The Council was formed to promote and protect democracy and human rights in Europe and can enforce international treaties - such as the ECHR - through the European Court of Human Rights in Strasbourg [23]. The principle legal body of the EU, responsible for enforcing most of the legislation discussed herein, is the Court of Justice of the European Union (CJEU) in Luxembourg.

The proliferation of information and communications technologies in the 1960s and 70s prompted a re-evaluation of the protections offered by these early instruments. The ECHR term 'private life' was judged to have several limitations: it did not clearly distinguish between privacy and protection of personal information and it emphasised protection from government and public bodies rather than private organisations [24]. Devised well before the widespread use of computers and electronic data processing, it also failed to adequately recognise the potential risk to privacy these presented [25, 26].

2.3 Early British Thought

In the UK, growing concern over the quantity of personal information held by organisations lead to two important reports in the 1970s: *The Report of the Younger Committee on Privacy* [27] and *The Report of the Lindop Committee on Data Protection* [28]. Tasked to consider whether new legislation was needed, [27] ultimately determined there was no requirement for a general privacy law. It did, however, recognise the potential for computers to adversely affect privacy and proposed ten overarching but non-binding principles [29, pp.517-8].

- The purpose of holding data should be specified.
- Only authorised access to the data should be permitted.
- There should be minimum holding of data for specified purposes.
- Persons in statistical surveys should not be identified.
- Subject access to data should be given.
- There should be security precautions for data.
- There should be security procedures for personal data.
- Data should only be held for limited, relevant periods.
- Data should be accurate and up to date.
- Any value judgements should be coded.

Clear similarities can be drawn between these and the principles forming the backbone of contemporary data protection laws [30]. Indeed, [25] observes that the later CoE convention discussed in section 2.4 was partially based on the Younger Report.

Though not enacted by the British government of the time, the report almost certainly influenced the government's later, albeit temporary, opinion that legislation and oversight may indeed be necessary. A 1975 *White Paper on Computers and Privacy* [31] observed: "the time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy" [25, p.2]. It identified five characteristics of computers that made them a threat to the privacy of personal information and which are equally valid today [32, p.243].

- They facilitate the maintenance of extensive record systems and retention of data in those systems.
- They can make data easily and quickly accessible from many different points.
- They make it possible for data to be transferred easily from one information system to another.
- They make it possible for data to be combined in ways which might not otherwise be practicable.
- They store, process and often transmit data in a form which is not directly intelligible.

Where the Younger Report addressed the more abstract notion of privacy, the Lindop Report focused on data protection and argued for the creation of an independent regulator. Again, government opposition to increased bureaucracy and cost meant its recommendations were not enacted. The report has been called a high watermark in the British government's enthusiasm for data protection. Even today it remains the UK's most comprehensive examination of the impact of personal data processing [33]. It can be argued the UK missed an opportunity to take a leading role in shaping international thinking on data protection. Instead, it would be European legislators that lead the way to Britain's first national data protection law [25, 32].

2.4 Council of Europe Convention 108

Enacted in 1981, effective from 1985 and extant today, the CoE *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108) [34], was the first legally binding international treaty on data protection.

The Convention defines personal data as "any information relating to an identified or identifiable individual" [34, p.2] and processing as any automated means of "storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination" [34, p.2]. It was the first legal instrument to define the concept of a data controller: "the natural or legal person, public authority, agency or any other body…to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied" [34, p.2]. Contrast between controllers and processors would come later. CoE members are required to take steps in their domestic law to give effect to the following seven principles [34, pp.3-4].

- Personal data should be obtained and processed fairly and lawfully.
- It should be stored only for specified purposes and not used in ways incompatible with those purposes.
- It should be adequate, relevant and not excessive for its stated purpose.
- It should be accurate and, where necessary, kept up-to-date.
- It should be stored in such a manner that permits identification of the data subjects for no longer than is necessary for its purpose.
- It should be protected from accidental or deliberate erasure, access, alteration or dissemination.
- Data subjects should have the right to know what data is held on them and be granted rights of correction or erasure as appropriate.

Art.6 also formalised the concept of the special categories of sensitive personal data which are exempt from processing unless domestic law provides 'appropriate safeguards'. As with later data protection guidelines, the terminology used is general and what constitutes 'appropriate' is not defined.

Art.12 imposes restrictions on transborder data flows to non-signatories where domestic laws do not provide equivalent protections. This prompted the UK government to reluctantly pass its own national

data protection legislation [25, 32, 33]. A government white paper observed: "[w]ithout legislation firms operating in the United Kingdom may be at a disadvantage compared with those based in countries which have data protection legislation" [35, p.2]. As we see in section 3.7.2, similar concerns will almost certainly influence the government following Brexit.

2.5 The Data Protection Act 1984

The Data Protection Act 1984 (DPA84) [36] was the UK response to the obligations imposed by Convention 108. It has since been wholly replaced by the DPA98 and a detailed discussion is unnecessary. Many of the provisions of DPA84 have been carried over to its successor, however, and a brief consideration provides some insight to how data protection has been viewed in a UK context.

As indicated previously, it seems the DPA84 was motivated largely by commercial concern rather than any genuine enthusiasm for data protection. Indeed, [33] points out that it was written to meet the requirements of Convention 108 at the most minimal level. It took no advantage of where the Convention set minimum standards but invited signatories to provide additional protections [33, pp.35-36]. Despite this, DPA84 did introduced significant changes to UK business practices. It established eight fundamental principles in line with those of Convention 108 and, indeed, those of the Younger Report. These are very similar to those of DPA98 and to prevent repetition are examined in section 2.6.

For the first time, data controllers were obliged to register and pay a fee to a new supervisory authority: the Data Protection Registrar (DPR), now the Information Commissioner's Office (ICO). Criminal charges and a tribunal were established for controllers who failed to register and for breaching the provisions of the Act [25]. A criticism of this model - which continues today - was that the DPR's only source of funding was the registration fees paid by controllers. This stemmed from a decision that the legislation should not impose a financial burden on the public purse and, arguably, suggests a lack of governmental commitment to data protection that endures today [33].

2.6 The Data Protection Directive 1995 and Data Protection Act 1998

By the early 1990s, it was becoming clear that Convention 108 was insufficient to deal with the increased capacity for personal data collection brought about by new technologies such as the Web and emergence of e-commerce. The period also coincided with the EU's growing confidence in imposing legislation on member states [37].

In this section, we examine the two principle legal instruments that define the current regulatory environment: the EU DPD95 and the UK DPA98. Once again, the UK government's intent with DPA98 appears to have been to meet the minimum standards of the European legislation. As such, the two are largely interchangeable in terms of scope and requirement [33]. Both are considerably larger than the legislation they supplant and both - the DPA98 especially - have a reputation for being too long, too complex and difficult to understand [38, 39]. Rather than examine each in isolation, our discussion encompasses both to present a hopefully clearer but somewhat simplified overview.

DPD95 was adopted in on 24 October 1995 to be implemented by 24 October 1998. It was the first EU legislation to regulate the use of personal data and had two primary aims [25, 37].

- To protect individual privacy in respect of processing personal data and foster the emerging digital economy.
- To harmonise laws across the EU and facilitate the transfer of personal data across national borders.

DPD95 applies to organisations established in the EU or that use equipment located within the EU [DPD95, Art.4(1a)]. This means the determining factor is the location of the equipment used to process data, not the location of data subjects. As we see in section 3.4.2, this is reversed under GDPR.

2.6.1 The Data Protection Principles

As a directive, DPD95 is not directly applicable but provides a framework of minimum standards for enabling national legislation. In common with most legal instruments on data protection it is underpinned by a set of basic principles. DPD95 contains six stated principles and discrete sections concerning the rights of data subjects and the export of data outside the European Economic Area (EEA). In DPA98, these are collated and presented as a set of eight principles which we briefly consider below.

Principle 1: Personal data shall be processed fairly and lawfully.

The first principle requires that controllers have legitimate grounds for collecting personal data and be transparent about how it will be used. In practice, this means informing data subjects that their data is being collected and why [40]. Also covered are the conditions for processing. In theory, these are limited to where the data subject has given their consent or where it is necessary [3, p.40]:

- for the performance of a contract to which the subject is party;
- for compliance with legal obligations;
- to protect the vital interests of the subject;
- to perform a task carried out in the public interest; or
- to meet the legitimate interests of the data controller, where such interests are not overridden by the interests and fundamental freedoms of the subject.

DPD95/DPA98 also recognise the special categories of personal data discussed in section 2.4 and place additional restrictions on their processing without the explicit consent of the subject or in other, clearly defined, scenarios. Neither ‘consent’ or ‘explicit consent’ are defined. Critics have pointed out that this imprecision has allowed organisations to take advantage of user apathy to obtain forms of ‘unambiguous consent’ that are clearly not in the spirit of the legislation, e.g. pre-ticked boxes accepting terms of service [38]. Consent is a major issue in GDPR and is discussed in section 5.2.

Principle 2: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

There is clear overlap between this principle and others, especially the first, so much so that [33] argues that it serves no effective purpose. Irrespective, [40] advises that organisations should adhere to the rules on notification and be clear from the outset the purpose of processing, ensuring any further processing is not incompatible with what the data subject can reasonably expect.

Principle 3: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

This principle is fundamentally about the practice of data minimisation. Controllers should hold only the minimum amount of personal data required for their purpose [40]. Although, technically, controllers can breach this principle by failing to hold enough data for the stated purpose, they are far more likely to breach the 'relevant' or 'excessive' aspects [25].

Principle 4: Personal data shall be accurate and, where necessary, kept up to date.

The fourth principle is largely self-explanatory, however, [40] observes that it may not be practical for controllers to confirm the accuracy of every piece of data received. Thus, DPD95/DPA98 merely require controllers take 'reasonable steps' to ensure the accuracy of data, consider any challenges by data subjects and, if necessary, consider updating the information. What constitutes 'reasonable' is, of course, a perennial legal debate. The term is not further defined in either legislation.

Principle 5: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The fifth principle is another example of where legislation provides little clarity in respect of controllers' obligations and there are no concrete minimum or maximum retention periods. What advice exists suggests that controllers regularly review their data holdings, consider the purpose of its retention and judge whether it is still necessary [40]. Unneeded data should be deleted, although the act of deletion also constitutes processing and so it must be completed in line with the other principles, notably the seventh which requires that it take place in appropriately secure circumstances [25].

Principle 6: Personal data shall be processed in accordance with the rights of data subjects.

In contrast with previous instruments, the current legislation codifies the rights afforded to data subjects. The most important of these are [3, 41]:

- the right of access to personal data at reasonable intervals and without excessive delay or expense;

- the right to have incomplete or inaccurate data rectified or erased;
- the right to prevent processing of personal data where the objection is justified;
- the right to prevent personal data being used for direct marketing;
- the right not to be subject to a decision that has legal effect that is based solely on the automated processing of data; and
- the right to claim compensation for damages caused by a breach of the rules.

GDPR introduces several changes to the rights of data subjects, the most important of which are discussed in Section 5.6.

Principle 7: 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.

Neither DPD95 or DPA98 give any clear direction apropos of the seventh principle. Where security is mentioned at all, guidance is limited to noting: "the controller must implement appropriate technical and organizational measures to protect personal data…[h]aving regard to the state of the art and the cost of their implementation…[and]…appropriate to the risks represented by the processing and the nature of the data to be protected" [2, p.43].

Linked to this, DPD95 was the first legal instrument to recognise the distinction between controllers and processors, the latter defined as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" [DPD95, Art.2(e)]. The onus is placed on controllers to ensure that any handling of personal data carried out by processors under their direction are in line with the principles [2, p.43]. Thus, under the current regime, controllers are held responsible for any breach caused by processors under their direction. The provision of security is an area in which GDPR offers greater clarity and is discussed in section 5.3.

Principle 8: 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.

The final principle prohibits export of personal data outside of the EEA unless adequate safeguards are in place or by consent of the data subject. The European Commission (EC) has so far issued eleven adequacy decisions: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Mann, Israel, Jersey, New Zealand, Switzerland and Uruguay [42].

Transfers to the United States, which has no general data protection law, was subject to special dispensation under the Safe Harbour agreement. This was a set of voluntary standards against which US organisations could self-certify [30]. Following the revelations made by Edward Snowdon in 2013, however, it became apparent that the US intelligence community had routine access to European personal data. The result was that in October 2015, the CJEU ruled Safe Harbour invalid [43, 44]. In

July 2016, it was replaced by the EU-US Privacy Shield agreement although this too is subject to criticism and ongoing challenge [45].

2.6.2 Plus ça Change

It should now be clear that there is a distinct pattern in the principles of the various instruments discussed so far. There is little material difference between the principles discussed above and those proposed in the Younger Report of 1972. CoE Convention 108 was based in part on the Younger Report; DPD95 was based in part on Convention 108; DPA98 is based almost entirely on DPD95 and, as we will see in part 3, GDPR is an expanded version of the preceding Directive. Thus, it is not so much what must be done that has evolved over the last four decades, rather how it should be achieved and the repercussions for failing to comply. This observation supports one of the key argument of this report: GDPR is evolutionary, not revolutionary.

2.6.3 Supervisory Authorities and Guidance

DPD95 introduced a requirement for each EU member state to establish an independent Supervisory Authority (SA) to control and monitor the processing of personal data. In the UK, this function is performed by the ICO. Art.24 obligates SAs to impose sanctions for infringements but is silent apropos of their nature or scale. Options available to the ICO include enforcement (cease-and-desist) notices, the imposition of regulatory audits and monetary penalties of up to £500,000 [46]. Over time, this lack of clarity in the Directive has led to variation between member states. In Germany, for example, breaching the Federal Data Protection Act carries fines of up to €300,000 while Italian courts can impose penalties of €1.2m [47].

Data controllers must notify the SA of each member state in which they wish to operate and provide details of their planned activities [DPD95, Art.18]. The value of this requirement has been subject of much scepticism. [38] argues that many organisations have simply lost track of the types of processing carried out by their staff and on what data. Thus, notification is made using broad and sweeping categorisations of the data to be collected and the intended processing, rendering the requirement a mere compliance function carried out for its own sake rather than any useful purpose. In the case of the UK, [33] suggests that the only clear purpose of the notification requirement is to provide the ICO's sole source of revenue for data protection activities. The requirement to notify is an important change - and has implications for ICO funding - which we discuss further in Section 5.5.1.

Finally, Art.29 of the Directive established the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (WP29), made up of a representative of the SA of each member state, the European Data Protection Supervisor (EDPS) and the EC. It acts as an independent advisory body offering guidance on data protection matters [48]. While not legally binding, the advice of the WP29 is taken seriously throughout the EU and is influential with SAs, including the ICO [25]. With the adoption of GDPR in May 2018, the WP29 will become the European Data Protection Board (EDPB) [49]. The group continues to issue guidance on key aspects of GDPR and its work is referenced throughout the remainder of this report.

2.7 Summary

This section has provided an overview of European and UK data protection policy: its origins, how it has evolved and where it now stands. Privacy and the protection of personal data is a fundamental right. Although the UK has historically been a reluctant adopter of European data protection laws, we note that its early work was influential in the development of those laws. It should be clear than the observations and principles formulated over 40 years ago are similar to those in place today and, as we see in the next section, those of the future.

PART 3: GDPR OVERVIEW

3.1 Introduction

In this section, we begin our examination of GDPR itself: its motivation, goals, scope and principle requirements. This informs the comparison between the DPD95/DPA98 and GDPR presented in part 4. We also provide clarity on GDPR's applicability to SMEs and discuss the issue of Brexit.

3.2 Problems with the Current Regime

DPD95 was intended to harmonise data protection across Europe. It has never been fully successful in this regard and discrepancies between member states make pan-European compliance a challenge [37]. Over time, a situation has arisen where no two domestic laws are sufficiently aligned for an organisation to be simultaneously compliant in its home country and all other 27 members. Thus, to maintain the free flow of information, governments and industry have had to implement bespoke processes - e.g. contractual clauses and Binding Corporate Rules (BCRs) - for handling an increasingly diverse array of scenarios [44, 50].

DPD95/DPA98 are also complex and often misunderstood pieces of legislation, supplemented by hundreds of amendments, recommendations and a near-constant stream of advisory documents from the WP29 and ICO. This is partly a matter of inopportune timing. The DPD95 was proposed in 1992, only three years after the 1989 invention of the Web by Tim Berners-Lee. In 1995, the global internet population was around 16 million [51] with fewer than 1% of Europeans using it regularly [52]. It can be argued that the Directive was based on a model of data processing that no longer exists: one that assumed most organisations would have only a few computers accessed by a limited, more easily controllable, number of staff. This is, of course, no longer the case: organisations have access to more data than ever before and employees can conduct processing operations with far less centralised control [38, 44, 53]. Today, internet penetration is Europe is over 80% [51] and the advent of e-commerce, social media, mobile devices and organisations whose very raison d'être is to process data means the CJEU has sometimes had to be creative in its interpretation of the law [26].

3.3 Goals of GDPR

In 2009, the EC launched a review that would eventually become GDPR. It cited the need to protect the fundamental right of privacy and bring the law up to date with the challenges of rapid technological development [54]. The GDPR can be said to have four primary goals.

- **To harmonise data protection laws across the Europe.** As a regulation, GDPR applies directly and enters force simultaneously throughout the EU [55]. States need not pass enabling legislation and its application needs no interpretation by national governments: scope for local variation is specifically identified [56]. This consistency is a key component of the EU's digital single market, enabling free movement of goods, services and information [57, 58].

- **To strengthen individual rights.** GDPR clarifies existing rights and establishes new ones to consider technological developments and improve consumer confidence in e-commerce. A 2015 survey2 [59] found a majority (71%) of EU citizens feel disclosing personal information is an unavoidable part of modern life, however, many (67%) are concerned about not having control of their data and fewer than half (37%) trust online businesses to protect it. Chief concerns cited include becoming a victim of fraud and personal data being used without the subject's knowledge or for purposes other than those for which it was provided. In other words, peoples' primary concerns are little different that those that motivated the early data protection measures discussed in part 2. [6] observes that such concerns can lead to a slow-down in the adoption of new technological innovations and a loss of new business opportunities. Conversely, increasing individual control over data enables trust and encourages economic activity.

- **To improve the effectiveness of enforcement and provide increased clarity for business.** GDPR substantially increases the role and powers of national SAs to help ensure compliance with best-practice [Art.58]. It also introduces new measures for international cooperation and coordination, such as the concept of a one-stop-shop for organisations operating internationally [56].

- **To enhance the protection of personal data transferred outside the EU.** GDPR seeks to streamline and improve procedures for international transfers of personal data while maintaining protection [54]. Driven by its extraterritoriality, GDPR aims to promote data protection at a global level [Art.70(w)] acting as a kind of 'gold-standard' for governments and industry [60].

3.4 Scope of GDPR

3.4.1 Key Definitions

Before addressing the requirements of GDPR, it is necessary to define some key terms. The GDPR defines personal data as:

> [I]nformation relating to an identified or identifiable natural person…who can be identified, directly or indirectly…such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity... [Art.4(1)]

For clarity, 'natural person' means a human being, as opposed to 'legal person' which refers to a company or organisation. This definition is more expansive than DPD95/DPA98 which, for example, make no mention of online identifiers. Indeed, GDPR specifies that IP addresses and cookies may qualify as personal data if they can be combined with other information to create profiles on individuals

[2] 28,000 EU citizens.

and identify them [Rec.30]. This has already been examined in the courts [61] and could affect organisations like Communications Service Providers (CSPs) and advertisers, both of whom routinely log such information about users.

Like DPD95/DPA98, GDPR recognises sensitive personal data to which greater protections apply. These are defined as:

> [P]ersonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership…genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. [Art.9(1)]

This definition is broadly like that of DPD95/DPA98 with the notable addition of genetic and biometric data where that data is used to uniquely identify an individual. This has potential consequences for the emergence of certain types of user authentication technologies [62], e.g. the voice recognition solution (Voice ID) used by the British bank HSBC [63]. The definition of processing is also expanded to include:

> [A]ny operation or set of operations which is performed on personal data…whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. [Art.4(2)]

The scope of this definition leaves little room for misunderstanding. Put simply, if an organisation is in possession of personal data, even in paper form, then it is almost unavoidably engaged in processing.

GDPR recognises two entities involved in handling personal data: controllers and processors. The definitions of these entities are effectively identical to those under DPD95/DPA98, i.e. a controller "determines the purposes and means of the processing of personal data" [Art.4(7)] and a processor "processes personal data on behalf of the controller" [Art.4(8)]. Where GDPR differs from current legislation is in the responsibilities placed of each, as discussed in part 5.

3.4.2 Territorial Scope

There is some confusion regarding the territorial applicability of GDPR and to whose data, exactly, it offers protection. [64] and [65], for example, describe the Regulation applying to EU citizens while others [50] suggest it applies to all EU residents including, e.g. refugees, visitor and those with working visas. This confusion is not helped by the fact that the words 'citizen' or 'resident' appear nowhere in the articles of the GDPR. Only in the recitals is the matter addressed: "[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence" [Rec.14]. Thus, the Regulation applies to all organisations located within the EU even if the data they are processing belongs to non-EU nationals who may be physically located elsewhere. This is a reversal of

the DPD95 and focuses on the location of data subjects rather than that of processing [44].

The recitals also provide guidance for organisations established outside the EU. Rec.23 states: "the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services…irrespective of whether connected to a payment." Rec.24 states: "[t]he processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union."

[66] interprets these requirements as meaning GDPR will apply to all organisations established within the EU and involved in processing personal data, even where such processing occurs outside the EU. Moreover, the Regulation will apply to organisations established outside the EU that target consumers inside the EU or monitor individuals' behaviour that takes place within the EU, including for advertising purposes. To summarise, the following rule of thumb may be applied: if either the data controller/processor or the data subject are located within the EU, any personal data processed is within scope of GDPR.

3.5 GDPR Data Protection Principles

GDPR is underpinned by a set of fundamental principles that set out organisations' main responsibilities. These are broadly like those required by DPA98 but with some important changes. Art.5(1a-f) states that personal data shall be:

- **(a) "[P]rocessed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')."** Rec.39 explains that to meet this requirement, data subjects must be informed, using clear and plain language, of information such as the identity of the data controller and the purpose for and extent to which their personal data will be subject to processing. This relates to the issue of consent and is examined in section 5.2.

- **(b) "[C]ollected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… ('purpose limitation')."** This is similarly worded to DPA98, although GDPR goes into greater detail regarding additional processing permitted in certain situations, e.g. historical or scientific research and statistical purposes. This is permissible where appropriate safeguards are in place, including pseudonymisation or other method that "does not permit or no longer permits the identification of data subjects" [Art.89(1)].

- **(c) "[A]dequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."** Minimisation requires "ensuring that the period for which the personal data are stored is limited to a strict minimum…[and]…time limits should be established by the controller for erasure or for a periodic review" [Rec.39]. This

principle - which necessitates understanding what personal data is held, for what purpose and for how long - could be a significant challenge [64, 67]. We return to this issue in section 5.5.

- **(d) "[A]ccurate 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')."** This principle builds on its equivalent in DPA98, especially regarding the enhanced rights to rectification and erasure under Arts.16 and 17 respectively. In the case of such requests, data controllers have one month to act, extensible by two further months depending on the complexity or quantity of requests [Art.12(3)].

- **(e) "[K]ept 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… ('storage limitation')."** As with the data minimisation requirement described above, this may present a challenge to organisations who may not be fully aware of their holdings of personal data. This is discussed in section 5.5.

- **(f) "[P]rocessed 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')."** While the legislation seeks to be largely non-prescriptive in terms of specific security technologies, encryption and pseudonymisation are defined as appropriate safeguards for protecting personal data [Art.32]. We discuss security in section 5.3.

Readers familiar with DPA98 will note the absence of principles relating to the rights of data subjects (the sixth principle of the UK Act) or international transfer of personal data (the eighth principle of the UK Act). These issues - both key aspects of GDPR - are addressed under Chapters III and IV of the Regulation respectively. Increased data subject rights are discussed in section 5.6. Finally, GDPR introduces an entirely new principle in Art.5(2).

- **"[T]he controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."** This requires that controllers can show *how* they comply with the principles defined in Art.5(1) above. Organisations will need to maintain detailed records that evidence their compliance with GDPR, including the processing activities under their responsibility, technical, procedural and organisational security measures and transfers of personal data to third countries [66]. Many organisations must also appoint a Data Protection Officer (DPO) to inform and advise their activities and Data Protection Impact Assessments (DPIAs) – risk assessments focusing on the privacy of personal data - become mandatory in some cases [Art.39]. The accountability principle is a major component of the GDPR and could represent a significant challenge for some organisations. This is discussed further in section 5.5.

3.6 Clarifying Applicability for Small to Medium Enterprises

Data protection and GDPR have become a headline topic for the boards of many large organisations. A March 2017 survey[3] [68] of large organisations revealed 81% considered GDPR compliance to be a major concern. Another survey [69] of Chief Information Security Officers (CISOs) in the financial sector found 52% viewed GDPR compliance as an investment priority over the coming year. While most large organisations are at least aware of GDPR, some smaller businesses are either unaware or wrongly believe they are exempt [8, p.14]. As recently as February 2017, a survey[4] [11] found 84% were unaware of GDPR. Separately, a small proportion (8%) believe the Regulation only applies to large, multinational organisations [70].

This confusion is not helped when a great deal of online information - often from apparently reputable sources - is either outdated or at least partially incorrect. For example, [71] states: "the Regulation must be observed by any organisations with more than 250 employees…[unless]…it's involved in processing of certain categories of personal data…" In other words, [71] suggests that SMEs must only observe GDPR if they are involved in processing sensitive personal data. This advice is incorrect or, at the very least, incomplete but widely repeated [e.g. 72, 73]. In reality, the only derogation offered to organisations with fewer than 250 employees is that they need not maintain the detailed records of processing activities required by the accountability principle. Even this exemption is void if such processing is considered high-risk, involves sensitive data or forms part of that organisation's core business [Art.30(5)]. In other words, the determining factor is the nature and scale of processing, not the size of the business.

Another common misconception [74, 75, 76] is that SMEs need not appoint a DPO. This is more understandable as an early draft of the Regulation did state: "SMEs are exempt from the obligation to appoint a [DPO] insofar as data processing is not their core business activity" [58]. This provision has since been rescinded and a DPO is required for all controllers and processors whose activities involve "regular and systematic monitoring of data subjects on a large scale" [Art.37(1)]. Again, it is the scale of processing, not the business, that is important. This was made clear by the ICO's Senior Technology Officer in June 2017: "I've heard plenty of people talking about there being a DPO exemption for SMEs. This is absolutely not the case" [77].

3.7 The Question of Brexit

In March 2017, the British government signed Art.50 of the *Treaty on European Union*, beginning a two-year period of negotiations prior to Brexit in March 2019, ten months after the implementation of GDPR in May 2018 [78].

[3] 900 organisations with at least 1,000 employees.
[4] 1,000 respondents from UK small businesses.

3.7.1 Brexit Confusion

In the months following the vote to leave, many businesses have voiced confusion over how GDPR would apply, if at all [79, 80, 81]. Despite confirmation [82, 83, 84] that GDPR will be introduced as planned - the UK will still be an EU member in May 2018 - confusion remains, especially among SMEs. A June 2017 survey[5] [70] found almost half (46%) of those subject to GDPR were uncertain if they would have to remain compliant after Brexit and some (6%) were convinced that they would not. Moreover, 20% of businesses surveyed had not yet begun preparations and a majority (71%) had budgeted no extra resources. As an aside, a small majority (51%) also did not believe their business was at risk of cyber-attack: a reminder of the misconception among many SMEs about the threat and need for appropriate safeguards.

Some sources indicate that confusion is not limited to the smallest organisations. A separate March 2017 survey[6] [85] found that almost a quarter (24%) had stopped GDPR preparation because of Brexit, 6% had not begun preparing at all and almost half (44%) believed that the Regulation may not apply post-Brexit. While these results appear to agree with [70] and the survey was cited widely [85, 86, 87], the raw data could not be obtained or verified. If the results are to be accepted, however, it seems reasonable to assess that confusion still abounds in some quarters. As observed by the Deputy Information Commissioner, Steven Wood: "uncertainty isn't good because it can delay investment in [GDPR] compliance systems" [88]. It seems clear that there is a need for stronger messaging from the government, ICO and industry leaders.

3.7.2 GDPR Means GDPR

Recent developments have provided some much-needed clarity. Introduced to parliament on 13 July 2017, the *European Union (Withdrawal) Bill 2017-19* [89] states: "[d]irect EU legislation, so far as operative immediately before exit day, forms part of domestic law on and after exit day" [89, p.2]. In other words, everything that is law the day before Brexit - including GDPR - will continue to be law the day after Brexit, at least in the short term.

In June 2017, the UK government announced a domestic equivalent of GDPR to replace the existing DPA98 [90]. The new Data Protection Act (DPA) will:

> Make our data protection framework suitable for our new digital age, allowing citizens to better control their data…implement the [GDPR]…meeting our obligations while we remain an EU member state and helping to put the UK in the best position to maintain our ability to share data with other EU member states and internationally after we leave the EU…[and]…update the powers and sanctions available to the Information Commissioner. [5, p.46]

[5] 501 organisations with 10 – 249 employees.
[6] 408 IT decision-makers in organisations of 100 - 1,000 employees.

There is, therefore, little room remaining for uncertainty: GDPR will be in force while the UK remains a member of the EU and the new DPA will take over following Brexit [91]. Although full details of the new Act have not yet been announced, [5, p.16] notes that it will: "strengthen rights and empower individuals to have more control over their personal data including a right to be forgotten when individuals no longer want their data to be processed". The mention of the right to be forgotten is a clear nod to GDPR. Together with references to 'international data sharing' and fines of up to £17m [92], it is judged highly likely that the new DPA will seek to match GDPR at a fundamental level, offering UK citizens the same protections as the European legislation.

The alignment between GDPR and the proposed DPA is likely to be a key factor in the UK government's strategy for maintaining commercial access to the European digital economy. Any country not a member of the EU or EEA is classed as a 'third country' to which transfer of personal data is only permitted when an adequate level of protection is guaranteed [93]. Although there are mechanisms that enable this for individual organisations (e.g. contractual clauses and BCRs mandating appropriate safeguards), an 'adequacy decision' granted by the EC is the most straightforward as it would apply to all UK organisations [94]. Thus, it is considered highly likely that the government's objective in specifying the new DPA is that it should meet the EC's requirements. Whether this can be achieved before Brexit is a matter of debate. Some experts believe the lengthy legislative process of making adequacy decisions - only eleven have been granted [42] - render it unlikely and note it could take "many, many years" to achieve [95, p.5]. The Information Commissioner, Elizabeth Denham, has acknowledged that "[a]chieving adequacy on day one after exiting the EU may be challenging…[but]…[i]f there is a way to negotiate either a transition arrangement or something so that there is not a cliff edge on day one, that is in the best interests of everybody" [96, p.4]. As observed by [62], if the post-Brexit UK were to remain in the European single market, it is likely that the requirements of GDPR will continue to apply fully.

A potentially critical factor in the UK's ability to obtain an adequacy decision is the introduction of the *Investigatory Powers Act 2016* (IPA16). Adopted in November 2016, the controversial Act [97, 98, 99] gives the UK intelligence and security community broad electronic surveillance powers and, in its original form, would have compelled CSPs to retain communication records for 12 months. This latter provision has since been deferred [100, 101] after a CJEU ruling that indiscriminate retention of data is unlawful [102]. As per section 2.6.1, similar concerns lead to the invalidation of the EU-US Safe Harbour initiative [43]. It seems possible that these concerns may also apply to any evolved form of the IPA16, possibly requiring a specially crafted agreement between the UK and EU.

To summarise, UK industry must recognise - and quickly - that the GDPR will be implemented and serve as primary legislation in the UK until at least March 2019. Beyond this, the announcement of a new DPA does not mean organisations will be released from its obligations. The two laws will almost certainly be inextricably linked and many organisations will be affected by both. Businesses operating solely within the UK with UK personal data will fall under the jurisdiction of the DPA; those operating internationally within Europe (or processing the data of EU residents) will also be bound by the extra-territoriality of the EU Regulation. In short, GDPR means GDPR.

3.8 Summary

GDPR represents an inevitable and much needed update to data protection law. We note, however, that the changes introduced are not ground-breaking and represent an evolution of the existing requirements. While the Regulation is largely intended to provide greater assurance to data subjects, there are also benefits for business, especially those involved in processing personal data in several European countries. Acting as something of a legislative 'reset button', GDPR realigns the current patchwork of national legislations, offering organisations greater clarity and assurance in respect of their obligations. Finally, this section clarified the position of SMEs and British business more generally following Brexit.

PART 4: COMPARISON AND KEY CHANGES

4.1 Introduction

Parts 2 and 3 presented an overview of the current data protection framework and GDPR. At a high level, the fundamental principles are broadly similar albeit expanded in some areas. It is fair to say that GDPR is significantly more detailed than its predecessor, stretching to 88 pages, 99 articles and 173 recitals compared with DPD95's 20, 34 and 72 respectively. The aim of this project is not to provide an exhaustive guide to GDPR but highlight key changes and how organisations may prepare. Thus, the purpose of this section is to provide a comparison and synthesis of the old and new requirements. Those judged most significant will form the bulk of discussion in the latter portion of this report.

4.2 Differences in the Principles

As per section 3.5, the principles underpinning GDPR are, for the most part, like those of the legislation it supplants. We note the following key changes.

- The first principle (lawfulness, fairness and transparency) is expanded to include a requirement for transparency of processing.
- The third principle (data minimisation) is expanded to provide clearer guidance apropos of what constitutes acceptable minimisation.
- The fourth principle (accuracy) is expanded to encompass the additional rights granted to data subjects in respect of rectification and erasure under Arts.16 and 17 respectively.
- The sixth principle (integrity and confidentiality) is largely analogous with the seventh principle of the DPA98 (security). We observe, however, the key difference that encryption and pseudonymisation are specifically highlighted as being of value in protecting data [Art.32] and can obviate the notification requirement following a personal data breach.
- The seventh principle (accountability) represents the greatest difference between the underlying requirements of GDPR and the previous legislation. It is an entirely new principle and means data protection is no longer simply a matter to be dealt with after a breach has occurred. Senior management must demonstrate their consideration of data protection throughout the information lifecycle.

4.3 Differences in the Definitions

Apropos of the definitions used in GDPR, we observe only three changes directly relevant to our discussion.

- The expansion of the definition of personal data to include location data and online identifiers [Art.4(1)].

- The expansion of the definition of sensitive data to include genetic and biometric data where that data is used to identify an individual [Art.9(1)].
- The strengthening of the definition of consent to include the requirement that it should be given by "clear affirmative action" [Art.4(11)]. This contrasts with the more ambiguous definition of "freely given specific and informed indication" [DPD95, Art.2(h)] which allowed subject inaction to qualify as consent in some cases.

All other definitions in GDPR are either largely synonymous with those in DPD95/DPA98 or are introduced for the first time, considering the additional scope of the Regulation. Where relevant, they are introduced as required in later sections of this report. A full listing of definitions is presented in Art.4 of the Regulation.

4.4 Differences in the Requirements

While the differences between the principles and definitions of GDPR and earlier legislation - excepting the new accountability principle - are relatively modest, the Regulation does introduce several more significant changes. Some of these, e.g. the scale of sanctions available to SAs, have been well documented while others are less well understood. Table 1 sets out these key changes, comparing the existing requirements with those of GDPR. Comparison is often draw between GDPR and DPD95 rather than DPA98. This is a matter of convenience as the two EU laws are more easily compared. The DPA98 is sufficiently close to DPD95 for the comparison to be valid. Table 1 is broken down into the seven categories below. These are used as a matter of convenience and do not appear in GDPR itself.

- Scope and extra-territoriality.
- Consent.
- Data processing.
- Security.
- Compliance.
- Data subject rights.
- Enforcement and penalties.

Table 1. Comparison of requirements between DPD95/DPA98 and GDPR

Category	Provision	DPD95/DPA98	GDPR
Scope	Territorial Scope	Determined by the location of the equipment used to process personal data. This includes organisations established in the EU as well as those using equipment located within the EU to process personal data [DPD95, Art.4(1a)].	Applies to processing carried out by all controllers *and* processors located within the EU [Rec.23] as well as those outside the EU to the extent that processing relates to offering goods and services or monitoring the activity of data subjects within the EU [Rec.24]. Thus, the situation is reversed and the deciding factor becomes the physical location of the data subject, not the location of processing.

Category	Provision	DPD95/DPA98	GDPR
	Harmonisation	Intended to harmonise data protection laws throughout the EU [DPD95, Rec.7]. Divergence during the 22 years since its adoption means organisations operating internationally must comply with various, sometimes conflicting, national legislations.	Applies directly to all member states, providing a single set of rules for organisations to follow. There are limited areas where individual member states can derogate, e.g. age of consent for children [Art.8(2)]. These are clearly highlighted but make it unlikely that true harmonisation will be achieved [56].
	One-Stop-Shop	Controllers required to notify and register with the SA of each EU state in which they operate [DPD95, Art.4(1a)]. Organisations operating internationally may have to coordinate with several SAs.	Introduces the concept of a one-stop-shop for cross border processing. Processing supervised by the 'lead SA', the authority of the member state in which the controller or processor has its main establishment [Rec.94].
Consent	Consent	Subjects must give their consent for processing unless it is required for specific purposes, e.g. execution of a contract with the data subject or for legal purposes. Lack of clear guidance on what constitutes adequate consent has resulted in implied or 'opt-out' consent in some cases where inaction is deemed to clearly signify consent, e.g. pre-ticked box [103].	New restrictions where a controller relies on subject consent to process data. • Consent must be made by clear, affirmative action with pre-ticked boxes specifically excluded [Rec.32]. • Where processing has multiple purposes, consent must be given for each [Rec.32]. • Consent document (e.g. privacy policy) must use clear, concise language and not be overly disruptive to the use of the associated service [Rec.32]. • Consent can be withdrawn at any time and it must be as easy for data subjects to withdraw consent as to give it [Art.7(3)]. Consent is discussed further in section 5.2.
Data Processing	Obligations for Controllers and Processors	Processors have only an indirect duty based on contractual obligations with controllers [105, 106]. Should a breach occur the controller, not the processor, is subject to sanction [107].	Processors now have legal liability. Although controllers retain the main compliance responsibilities, processors have direct obligations in areas such as security, accountability and breach notification [106]. They are obligated to implement appropriate security measures [Art.32] and may be liable for damages caused to data subjects following breaches of the Regulation [Art.82(2)].

Category	Provision	DPD95/DPA98	GDPR
	Protection by Design and Default	No reference to 'data protection by design or default', only "appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself…in order to maintain security and thereby to prevent any unauthorized processing" [DPD95, Rec.46]. Thus, the focus is on the security rather than nature of processing.	As per the accountability principle, organisations must demonstrate that they have considered and integrated data protection. Specific measures, e.g. encryption and pseudonymisation, are suggested as appropriate controls for achieving this [Art.25]. Organisations will have to consider data protection from the outset during development of new processes or applications [50]. This is discussed in section 5.5.3.
	DPIAs	No general requirement for DPIAs. During notification controllers must provide a "general description allowing a preliminary assessment to be made of the appropriateness of the measures taken…to ensure security of processing" [DPD95, Art.19(1f)]. Although not mandatory, the ICO promotes DPIAs as best practice [104].	Where processing involves 'high-risk' to data subjects, e.g. new technologies, the controller must conduct a DPIA and consult the SA before processing begins [Art.35(1)]. GDPR makes mandatory what was already considered best practice. DPIAs are discussed in section 5.5.2.
Security	Security of Processing	Controllers must implement "[a]ppropriate technical and organisational measures…against unauthorised or unlawful processing…and against accidental loss or destruction of, or damage to, personal data." [DPA98, Pt.I(7)]. It is left to the controller to decide how much and what type of security should be provided.	Similarly open-ended apropos of its direction on security, however, Art.32 does provide greater guidance including the use of specific technologies, e.g. encryption and pseudonymisation. Security is discussed in section 5.3.
	Breach Notification	No specific requirement to notify SAs or data subjects in the event of a data breach [108].	Specific obligations on controllers and processors with respect to notifying the SA and, in some cases, data subjects. Controllers must notify the SA no later than 72hrs after discovery of any breach likely to adversely affect data subjects [Art.33]. Breach notification is discussed in section 5.4.

Category	Provision	DPD95/DPA98	GDPR
Compliance	Notification and Record Keeping	Organisations must notify the relevant SA in each EU state prior to processing. In some cases, e.g. DPA98, notification must be resubmitted annually [66, 109].	Obviates prior notification (or annual re-notification) unless processing is deemed 'high-risk' and, even then, only the SA of the organisation's main establishment must be notified [Rec.94]. Organisations must instead maintain detailed records of their processing activities to be made available to the SA on request [Art.30]. See section 5.5.1.
	DPOs	No requirements to appoint DPOs.	Many organisations, irrespective of size, must appoint a DPO, including all public bodies less courts acting in their judicial capacity and all private organisations where activity requires regular or systematic monitoring of data subjects on a large scale or processing of sensitive data on a large scale [Art.37].
Data Subject Rights	Increased Rights	Data subjects are afforded the right to [DPD95, 41]: • access personal data; • have incomplete or inaccurate data rectified or erased; • prevent processing where the objection is justified; • prevent personal data being used for direct marketing; • not be subject to decisions with legal effect based solely on automated processing; and • claim compensation for damages caused by a breach.	GDPR adopts all existing rights, expands some and introduces new ones to include the rights to [Arts.12-21]: • be informed that personal data is being collected; • access to personal data, which is broadly the same; • rectification of incomplete or inaccurate data; • erasure (to be forgotten) where there is no compelling reason for continued processing; • restrict processing of personal data, which is broadly the same; • data portability, i.e. to obtain, copy, transfer or reuse personal data easily; • object, which is an expansion of the right to prevent data being used for direct marketing; and • rights relating to automated decision-making and profiling, such as online tracking or behavioural advertising. Changes deemed most likely to impact on business operations are discussed in section 5.6.

Category	Provision	DPD95/DPA98	GDPR
Enforcement and Penalties	Administrative Fines	In the UK, the ICO can fine an organisation a maximum of £500,000. The largest fine issued to date is £400,000 [110].	Maximum fines range from €10m or 2% of global turnover (henceforth 'lower tier' penalties) to €20m or 4% of global turnover ('higher tier' penalties), depending on the offence [Art.83]. SAs are further endowed with wide powers beyond simple administrative fines.
	Compensation Claims	Individuals may pursue a claim of compensation if they have suffered 'damage'. Although 'damage' is not clearly defined, it is broadly suggested that mere 'distress' is not sufficient to bring a successful claim [DPA98, Pt.II(13)].	Individuals' are empowered to bring a claim for compensation for "material or non-material damage" [Art.82(1)]. Thus, individuals may be able to bring private claims against processors and controllers even where no clear financial loss has been suffered.

4.5 Summary

The elements of GDPR discussed in Table 1 are deemed to be those most significant for UK industry. Other changes do exist but are not subject to detailed discussion in this report. GDPR restates the core principles of earlier legislative instruments while building on areas such as individual rights, accountability and supervisory control. Some changes - while potentially costly, e.g. the need for DPOs - are relatively straightforward and need no detailed discussion. Others may require more fundamental changes in how organisations handle personal data.

PART 5: KEY IMPACTS AND CHALLENGES

5.1 Introduction

While the principles of GDPR are broadly like those of existing legislation, the Regulation does introduce new challenges for organisations. Some are restatements of existing requirements while others are entirely new. This report is not intended as an exhaustive guide to GDPR compliance and several of the better-known aspects of the Regulation are not examined in any depth. The requirement for certain organisations to appoint a DPO, while notable, is straightforward and clear guidance already exists [111]. Similarly, the scale of administrative penalties, while an obvious concern, requires no detailed analysis as these are clearly specified in the text itself [Art.83]. Instead, this section examines some of the less well understood or potentially challenging aspects including those concerning consent, security and breach notification, accountability and data subject rights.

5.2 Consent

Consent is a commonly used lawful basis for processing personal data. When someone clicks to accept a privacy policy they give their consent for the processing specified, whether they have read the document or not. This is considered a form of 'implied' consent.

Like DPA98, GDPR refers to both 'consent' and 'explicit consent' and, like DPA98, the difference between the two is not defined. Explicit consent is required for processing special categories of sensitive data [Art.9(2a)] or where automated processing is used to make decisions with legal effect [Art.22(2c)]. The ICO has issued draft guidance on consent [112] although this will not be finalised until the opinion of the WP29 is published in December 2017. In the meantime, it suggests "the key difference is likely to be that 'explicit' consent must be affirmed in a clear statement (whether oral or written)" [112, p.24]. Thus, a simple checkbox would not qualify unless it is presented alongside a statement that specifies the nature of the sensitive data and/or the details of the automated decision and its legal effect.

In the absence of final guidance, this section considers consent more generally, defined as:

> [A]ny freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. [Art.4(11)]

In other words, consent must be: (i) specific and informed and (ii) given by a clear affirmative action. In the case of the former, Rec.42 clarifies that: "[f]or consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended." Moreover, where processing has multiple purposes, Rec.32 requires that consent be given for each of them. Thus, controllers cannot simply request open-ended consent to cover any future processing [103]. Some controllers may have to re-write their privacy policies to meet this requirement.

Rec.32 clarifies that 'affirmative action' can include: "ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates…acceptance of the proposed processing." Notably, "[s]ilence, pre-ticked boxes or inactivity" cannot constitute consent [Rec.32]. This is a change from DPD95/DPA98 which permit implied or 'opt-out' consent in some cases where an action or inaction were deemed to clearly signify consent [103]. Organisations currently relying on this will have to re-obtain consent from their users. This is not required where existing consent already meets the standards of GDPR, although the Regulation also requires that all consent is documented and retained so there may still be work to do [112]. Failure to correctly obtain or manage consent can attract a higher tier administrative penalty [Art.83(5a)].

5.2.1 Withdrawal of Consent

GDPR allows individuals to withdraw their consent easily and at any time. Upon doing so, they may have the right to erasure and for their data to no longer be processed: the so-called 'right to be forgotten' [Art.17(1)], discussed in section 5.6.2. It must be as easy to withdraw as to give consent [Art.7(3)]. Users must be informed of this option and ideally withdrawal should available using the same method as it was given. Organisations may have to introduce new mechanisms to allow this, e.g. a preference-management tool for web-based services. Withdrawal is not retrospective and does not affect processing done up to that point [112].

5.2.2 Consent of Children

GDPR treats consent of children as a special case. Art.8 states consent is only lawful if the child is at least 16 years old, otherwise it must be granted by a parent or guardian. This may necessitate reliable age and identity-verification measures for many organisations and will be subject to future guidelines [112]. As per section 3.3, harmonising data protection across the EU is a primary objective of GDPR, however, age of consent is an area with allowance for variation. Individual nations may set a lower age of not below 13 years [Art.8(2)]. It is not yet clear how many states will implement a reduced age of consent, although the UK has already indicated it will do so [113]. This should simplify dealing with child consent – fewer users will qualify as a child - but such differences have the potential to create difficulties for organisations operating internationally, arguably reducing the benefit of harmonised legislation. Organisations must be careful not to be fooled by the appearance of a single, unified rule and take steps to ensure they are aware of any jurisdictional differences [66].

5.3 Security of Processing

GDPR obligates controllers to protect personal data. Where processing is carried out by a separate entity, "the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational [security] measures" [Art.28(1)]. For the first time, Art.32 also gives processors a legal - rather than contractual - obligation to protect data. This is a sensible evolution: in many cases a processor, e.g. cloud provider, will be better positioned and equipped to secure data than a controller, who could be an SME with limited security expertise [105].

Art.32(1) states controllers and processors must "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk." Critically, unlike a traditional security risk assessment, the risk relevant to GDPR is that affecting data subjects not the controller or processor [106]. GDPR is largely silent on how security is provided but does give some guidance, suggesting inter alia as appropriate [Art.32(1)]:

- pseudonymisation and encryption;
- ensuring ongoing confidentiality, integrity, availability and resilience of processing;
- the ability to restore availability in the event of a physical or technical incident; and
- implementing a process for regularly testing, assessing and evaluating the effectiveness of security.

5.3.1 Data Protection and Information Security

Art.32(2) emphasises taking a risk-based approach to prevent "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed." Readers familiar with information security will recognise such requirements. Indeed, if we replace 'personal data' with 'information' we end up with something largely synonymous with definitions of information security itself: "preservation of confidentiality, integrity and availability of information" [114, p.4] and "protection of information…from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" [115, p.64].

An argument can be made that the security requirements of GDPR are effectively identical to those of the information security function; only the nature of the data is different. As many data protection breaches are the result of security failures [116], it seems obvious that the two disciplines must work together. In larger organisations, where information security and data protection may operate in vertically segregated silos, personnel dealing with GDPR compliance (e.g. a legal department) may have insufficient understanding of or involvement with those dealing with the Information Security Management System (ISMS). This could mean the ISMS relies on a security policy based on a subjective risk assessment that considers only risks to the organisation and not data subjects. Such lack of cooperation could represent a serious structural weakness [117]. GDPR will require many organisations to rethink how they protect personal information. It presents an opportunity to drive convergence between information security and data protection in organisations that have traditionally viewed them as discrete entities.

While Art.32 is more detailed than previous legislation, is provides little concrete guidance for organisations trying to implement GDPR-compliant security. This shortcoming is partially addressed in the recitals. Rec.49 suggests mechanisms to provide access control, prevent malware, prevent or limit denial of service (DoS) and protect against physical attacks. Rec.78 requires that organisations implement internal technical and organisational measures to prevent unauthorised or excessive access to personal data. This could be a policy of restricting access on a need-to-know basis enforced through

adoption of a role based access control (RBAC) model [118]. Such advice is not new: the principle of need-to-know (or least privilege) has existed since before the EU even existed. It "limits the damage that can result from an accident or error…so that unintentional, unwanted, or improper uses of privilege are less likely to occur" [119]. It should be clear that implementing such controls falls under the remit of security practitioners rather than those dealing with data protection compliance.

5.3.2 Beyond Confidentiality

While long-standing security advice continues to be relevant, new technologies and working practices also represent a threat to the security of personal data. More than half (59%) of British businesses use cloud services and almost as many (46%) allow employees to use personal devices for work purposes (Bring Your Own Device or BYOD) [8]. Organisations must obtain assurances from providers of the former and apply suitable security controls on mobile devices in the latter. As per the accountability principle (see section 5.5), organisations must know what personal data they have and where it is located. Similarly, it is impossible to secure something without understanding its nature and location. Establishing this knowledge has potential business benefits and 52% of organisations believe the audits required to identify personal data will lead to their business data being better understood and controlled [12]. Thus, data protection and security have complementary requirements and should work together in preparing for GDPR.

It is perhaps natural that organisations focus on confidentiality when planning for GDPR. Personal data leaks are increasingly reported in the media [120] and no organisation wants to have such failings brought to public attention. It is important to remember, however, that GDPR does not equate security with confidentiality: integrity, availability and resilience are also required. This means contemporary threats like ransomware rendering data inaccessible also become a data protection concern [118, 121].

The May 2017 Wannacry ransomware attack affected large parts of the UK National Health Service (NHS). Many hospitals were unable to access patient records, although there is no indication that the records' confidentiality was affected [122]. Flowing the attack, the head of security for NHS Digital said: "if I am being honest there may be some [NHS] organisations that have corrupted backups…or don't have backups" [123]. A reliable backup strategy is a fundamental security control and its absence indicates a clear break between the security and data protection functions. As of August 2017, the ICO investigation is ongoing [124] but a reasonable interpretation of GDPR suggests the event would constitute a breach of the Regulation, especially if affected data cannot be recovered. That the data affected includes sensitive medical information, potentially affecting patient care, is an aggravating factor, especially as the NHS had been warned repeatedly that it may be susceptible due to its outdated IT infrastructure [125, 126].

Apropos of what constitutes 'appropriate measures', a reasonable rule of thumb might be that if the cost (in terms of money, time or effort) of a security control is less than the potential harm caused by a breach, not implementing that control could be viewed as a failure to act reasonably. Any measure of 'harm' could, of course, be highly subjective so a better approach might simply be to implement widely accepted best practice. For its part, the ICO advises adopting basic security practices such as anti-

malware, patch management, disabling unnecessary accounts and services, backups and user education [127]. Failure to do so could leave an organisation open to enforcement action. In recent months, the regulator has issued fined for failing to conduct adequate security testing [128], failing to perform timely patch management [129] and exposing sensitive personal data to publicly accessible web services [130]. In another example, the ICO fined an organisation for not physically protecting media holding personal data, resulting in theft of the equipment by an employee [131]. These are all examples of issues that might normally be viewed as the responsibility of the security function so increased cooperation will clearly be beneficial. The fines issued in the cases above are nowhere near the scale of those possible under GDPR, which provides for lower tier penalties for security failures leading to a breach [Art.83].

5.3.3 Perfect Security

While security is clearly important, GDPR does not demand perfect security. Rather, organisations must take a risk-based approach to implementing controls appropriate to the threat and the sensitivity of the data. Where this is demonstrated, there is no violation even in the event of a breach [105]. Assuming reasonable security measures generally, an organisation suffering a zero-day exploit, for example, is unlikely to be penalised [132]. Art.82(3) states: "[a] controller or processor shall be exempt from liability…if it proves that it is not in any way responsible for the event giving rise to the damage." It seems impossible for an organisation to provide such proof unless its data protection and security functions are well integrated.

The fact that GDPR provides little direct guidance on security controls is a strength. Instead of mandating mechanisms that might quickly be rendered obsolete, it provides for a minimum baseline. In other words, instead of specifying how data is protected it specifies the level of security to provide, leaving organisations free to choose the most appropriate controls [53]. Organisations can use adherence to approved codes of practice or standards to demonstrate compliance with GDPR's security requirements [133, Arts.40-42]. This may drive further adoption of risk-based standards such as ISO/IEC 27001 or others developed specifically for GDPR compliance [106].

5.4 Breach Notification

Cyber-attacks and data breaches are rapidly becoming a fact of life for many organisations. The 2017 Cyber Security Breaches Survey [8] found just under half (46%) of all British businesses had suffered a breach in the last 12 months. The same survey discovered 61% of all UK businesses hold customer personal data and those that do are more likely to suffer a breach (51% versus 37%). There is currently no express obligation to report a breach, meaning the true number may be higher than surveys indicate [37, 108].

Unlike DPD95/DPA98, GDPR provides a definition of what constitutes a personal data breach:

> [A] breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. [Art.4(12)]

[106] observes that this definition is sufficiently broad that any loss of security affecting personal data is likely to qualify. Controllers and processors have new legal obligations to report actual or suspected breaches [133]. For processors, this is relatively straightforward: "[t]he processor shall notify the controller without undue delay after becoming aware of a personal data breach" [Art.33(2)]. This is unlikely to cause much impact as similar contractual obligations likely already exist. The obligations for controllers are more onerous and consist of two categories: (i) notification to the SA and (ii) communication of a breach to the data subject(s).

5.4.1 Notifying the Supervisory Authority

On becoming aware of a personal data breach, "the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority" [Art.33(1)]. The notification should contain as much information about the breach as possible and at least [Art.33(3)]:

- the quantity and type of personal data and number of subjects affected;
- the DPO or other point of contract;
- the anticipated consequences; and
- measures taken or proposed to control the breach and/or mitigate its effect.

Controllers must also maintain a record of any personal data breaches suffered, however minor and whether notified or not, to be made available to the SA on request [Art.33(5)]. Clearly the 72-hour timeframe leaves little time so developing an efficient breach notification process will be an important aspect of organisations' incident response procedure [116]. At the very least, one of the first steps to take after the discovery of a breach should be to consult with the DPO and information security functions to determine what has happened and decide if notification is necessary [50]. Organisations should use technologies like intrusion detection and prevention systems to identify breaches as soon as possible [Rec.87]. In the case of complex breaches or ongoing incidents, it is acceptable to send an initial report followed by phased updates as information becomes available [77].

Controllers can take relief from the fact that there are exemptions in certain circumstances. If a breach is judged unlikely to result in risk to data subjects the controller does not have to inform the SA, although it must still be recorded [Art.33(1)]. This could be where data is judged sufficiently insensitive that damage is unlikely, e.g. a list of names without further detail. Similarly, if data is encrypted there is no need to notify the SA. Indeed, [50, 64] observe that GDPR should act as a significant driver in adoption of encryption for organisations that do not already use it. This may require a major operational change, however, as, according to [8], fewer than two-fifths (37%) of British businesses currently have rules around encryption of personal data.

5.4.2 Notifying Data Subjects

If a breach is judged to represent a high-risk to data subjects the controller must inform them individually. Unlike notification to the SA, there is no strict timeframe on this. It must be done without undue delay and in clear and plain language, including at least the information covered in the latter three points above [Art.34(1-2)]. The purpose is to allow individuals to take any steps necessary to prevent further damage, e.g. identity fraud or compromise of further personal data held on another service [Rec.86]. This has a potentially high cost to business, especially if the controller cannot determine which subjects are affected or has limited means of contacting them. Where the effort and expense of informing data subjects individually is considered disproportionate, Art.34(3c) permits use of a public communication, e.g. a newspaper advertisement or press release.

Controllers are not obligated to inform data subjects if data is encrypted or where subsequent actions have removed or mitigated the risk [Art.34(3b)], e.g. a lost laptop or mobile device that has subsequently been remotely wiped of all data [106]. Unfortunately, as with many aspects of the Regulation, the distinction of what constitutes low and high-risk is not clearly defined and many organisations may be unsure of whether to report a breach or not. Some sources argue that it is "good practice to make notifications by default in order to avoid accidentally breaking the law" [116, p.242], however, whether the ICO will have the capacity to deal with the volume of notifications resulting from this approach in is another matter. Implementing the measures needed to obviate notification (mainly encryption) would seem to be a more effective and sustainable approach.

5.5 Accountability Obligations

Perhaps the greatest change between DPA98 and GDPR is the introduction of the accountability principle: the requirement that organisations demonstrate how they comply with data protection rules. The Information Commissioner, Elizabeth Denham, described it as "about moving away from seeing the law as a box ticking exercise, and instead to work on a framework that can be used to build a culture of privacy that pervades an entire organisation" [134]. Organisations must dispense with the view that data protection is about mere compliance and failure can result in a fine even where no data breach has occurred.

The accountability principle introduces obligations for all organisations and additional requirements for those above a certain size or engaged in 'high-risk' processing. This section discusses several of the more notable aspects: documentation of processing activities, DPIAs and the requirement for protection by design and default.

5.5.1 Documentation of Processing

Art.30 requires that controllers maintain records of all processing activities that take place under their responsibility. These must include [Art.30(1)]:

- the type of data;
- the nature and reason for processing;
- recipients, including those in third countries, to whom the data has or will be disclosed;
- the envisaged timeframe for retention; and
- security measures in place.

Similarly, processors are required to maintain records of all processing carried out on behalf of a controller [Art.30(2)]. Records must be made available to the SA on request [Art.30(4)] and [50] notes the definition of 'processing' is sufficiently broad that virtually any contact with personal data will qualify and require documentation.

Organisations with fewer than 250 employees need not maintain records unless processing is deemed 'high-risk', frequent or involves sensitive data [Art.30(5)]. This provision appears to be the source of the confusion over the GDPR's applicability to SMEs discussed in section 3.6 and organisations must be careful that they do not incorrectly believe themselves to be exempt. [135] observes that the exemption is actually very narrow: processing must be 'occasional' to qualify but no further advice is offered to explain what this means. Organisations should retain professional or legal counsel before determining if they are exempt. Breach of the requirement can attract a lower tier penalty [Art.83(4)].

The requirement will create an obvious administrative burden. Businesses that operate using agile methodologies, relying on flexible decision-making and little documentation, could be particularly affected and may have to plan and adopt new working practices [136]. Organisations will be compelled to identify exactly what personal information they hold through a comprehensive data audit. This must address questions such as why and for how long the data has been held, the legal basis for processing and with whom has it been shared. This could be an enormous challenge since, as noted in [67], the boom in e-commerce, harvesting of personal information and new technologies like social media mean many organisations have simply lost track of their data holdings.

An interesting potential solution, yet to be explored in the academic literature, is whether organisations could implement a system like that used in the Payment Card Industry Data Security Standard (PCI-DSS) [137, 138, 139]. PCI-DSS places strict obligations on organisations who hold or processes payment card information. These including the creation of a segregated cardholder data environment and mandatory security controls including encryption, network security measures and access control [140]. Implementing a 'personal data environment' akin to that for cardholder data under PCI-DSS could help organisations keep track of the information they hold, where it is located and how it is processed. This presents a potentially novel avenue of further research, albeit one complicated by the far broader range of personal data that much be controlled.

Finally, it should be noted that the requirement to maintain records of processing does have a positive aspect for business. It obviates the general requirement under DPD95 for controllers to notify and register with the SA of each EU state in which they operate [66, 109]. Rec.89 observes that this obligation "produces administrative and financial burdens…[and]…did not in all cases contribute to improving the protection of personal data." Instead, organisations need only consult the SA of the state of their main establishment prior to beginning any 'high-risk' processing [Rec.94]. This is associated with the need for DPIAs and is discussed in the next section.

As an aside, the removal of mandatory notifications may have adverse consequences for data protection oversight in the UK. The annual notification fee levied on controllers by the ICO forms that organisation's only source of funding for data protection activities [141]. This stems from an early decision that data protection should not impose a burden on the public purse and, arguably, suggests a lack of governmental commitment to the concept that continues today [33]. Indeed, [141] suggests that the government should find a way of allowing the UK to retain the fee or introduce an alternative one, noting: "if the Government fails to achieve this, the unappealing consequence is that funding of the ICO's data protection work will have to come from the taxpayer" [141, p.3]. Thus, there is an open question on how the ICO will be funded after the introduction of GDPR and, in the absence of an alternative source, how effectively it could pursue breaches. The organisation's annual report for 2016/17 [142] notes only that it expects GDPR to require a 70% increase in its budget [142, p.54] and it is in the process of negotiating with parliament a new fee system to be in place by 2018/19.

5.5.2 Data Protection Impact Assessments

Where processing is deemed to involve 'high-risk' to data subjects, GDPR requires that the controller carry out a DPIA before it begins [Art.35(1)]. Confusion exists because GDPR does not explicitly define what kind of processing constitutes high, medium or low risk, nor does it explain how a DPIA should be carried out [135]. Examples given for when DPIAs are likely required include [Art.35(3)]:

- use of new technologies;
- where the product of processing is used to make decisions with legal effect;
- when processing sensitive data;
- when using automated profiling; and
- large scale monitoring of public areas, e.g. CCTV.

Organisations waiting for clarification from the WP29 may be disappointed. Guidance issued in April 2017 [143] stops short of providing a clear list of operations considered 'high-risk'. Instead, it gives examples of when a DPIA should be considered [143, pp.7-9].

- When evaluating or scoring data subjects, e.g. employee performance or assessment for eligibility for products such as insurance or credit.
- When using automated decision-making with legal or significant effect.
- Any systematic monitoring, including in respect of publicly accessible areas (e.g.

CCTV) or where data subjects may be unaware of processing or have no way of avoiding it.

- All processing relating to sensitive personal data or criminal convictions.
- Where data is processed on a 'large scale' in respect of the number of data subjects, quantity or variety of data and the duration or permanence of the processing.
- When datasets are matched or combined in a way that exceeds the reasonable expectations of data subjects, e.g. obtained by more than one controller.
- When processing data concerning vulnerable persons including children, the mentally ill, asylum seekers, the elderly or employees of the controller (who may be pressured into accepting monitoring).
- When using new or innovative technology, e.g. biometrics, big data analytics, embedded systems or Internet of Things (IoT) devices.
- Data transfers outside the EU.

Although there appears to be no concrete rule, it seems the more of the above factors are met, the more likely a DPIA is required. WP29 suggests processing that meets only one of the criteria may not require a DPIA, however "in cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law" [143, p.7]. GDPR allows SAs to specify situations in which DPIAs are required so this advice is pending further guidance from the ICO [50].

Ultimately, the aim of a DPIA is to determine whether the benefit of processing is justified against the potential impact to the privacy of data subjects. They should cover the nature of data to be processed and justification of its necessity and proportionality in respect to the legitimate interests of the controller. A DPIA should also consider the type and extent of potential risk to the privacy of data subjects and the measures the controller proposes to mitigate those risks [Art.35(7)]. Evaluations of any potential impact risk being an inherently subjective determination; organisations should ensure their decision is adequately justified and be prepared to defend it. A suggested model for carrying out DPIAs is presented in [143] with further guidance offered in [104]. Like any risk assessment, DPIAs are not static and must be periodically reviewed - at least every three years, according to [143] - to ensure that the risk has not changed and controls remain effective [Art.35(11)]. Finally, while DPIAs are a controller responsibility, they need not be conducted by the controller. In many cases, it may be advisable for them to be conducted by the processors actually handling the data [50].

Where a DPIA indicates a controller cannot adequately minimise risk due to technological limitations or cost, the controller should consult the SA [Art.35(11)]. One again, and with no universally accepted method of measuring risk, GDPR provides little guidance on what sort of processing might require prior consultation. [135] opines that without further direction, this question may remain open until actual cases have been considered by the ICO and courts.

DPIAs are not merely compliance functions. They allow organisations to demonstrate that appropriate measures have been considered to handle potentially risky processing and, as such, form an important

component of the accountability principle [143]. Although DPIAs are not a legal requirement under DPA98, the ICO has long promoted their use and considers them an important aspect of a privacy by design approach to data protection [104]. DPIAs have been required in the UK public sector for several years and are already widely used by many larger private enterprises. Thus, the main difference between GDPR and DPA98 is that DIPAs become mandatory, effectively formalising a process that was already considered best practice. SMEs - for whom the requirement is new - are likely to be among those most affected [135].

5.5.3 Data Protection by Design and Default

An aspect of the accountability principle that has caused some confusion is 'data protection by design and by default', which is addressed in Art.25. Protection by design concerns the specification of processing systems and requires that:

> [A]ppropriate technical and organisational measures…which are designed to implement data protection principles…in an effective manner and to integrate the necessary safeguards into the processing. [Art.25(1)]

Protection by default is concerned with how processing systems are used and how they treat personal data.

> [B]y default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. [Art.25(2)]

GDPR does not provide a clear explanation of what data protection by design and default entails in practice. This is understandable as the Regulation largely avoids mentioning specific technologies, presumably to avoid becoming quickly outdated. This will serve as little consolation to businesses that fall foul of the rules, however, as lower tier fines are available for infringing Art.25. Clearly then, it is necessary to better understand the scope and requirements of this obligation.

Protection by default is perhaps the more intuitive concept and can be specified as two discrete requirements: (i) only data required for a specific purpose is processed (in line with the minimisation and storage limitation principles) and (ii) personal data is not, by default, accessible to a wide audience. There are several possible steps: reviewing web-forms to ensure only genuinely necessary data are collected [144], applying encryption and pseudonymisation to personal data at rest or in transit [64] and ensuring that 'out-of-the-box' settings for a device, application or service are those offering the greatest level of privacy [145]. A social media service, for example, might set user profiles to 'private' by default and require a positive action to make their data viewable to others. While this seems common sense, it

is worth remembering that until 2014, all content posted to Facebook was fully accessible to the public by default [146].

Protection by design - often referred to as Privacy by Design (PbD) - is a less concrete concept and it is not immediately clear how its inclusion adds anything beyond the data protection principles themselves. At a high level PbD is relatively simple, requiring that privacy concerns are embedded into the development of a system or product from the earliest stages [147]. It has been criticised, however, for being vague and for placing too great an emphasis on system designers rather than entities that actually use a system to process data [148]. This is important because it is the data controller, not the system designer, that will be held liable for any breaches and many organisations purchase commercial off-the-shelf (COTS) products to carry out processing. Thus, the means of processing may effectively be determined by the design of systems over which controllers may have little influence [135]. Controllers will have to take steps to ensure any COTS products have appropriate safeguards in place before accepting them into service.

Other commentators suggest that the more literal interpretation of PbD - hard coding data protections rules into the fabric of a system - is flawed because of the number of potential variables and lack of a 'one-size-fits-all' solution. Instead, development of a 'privacy mind-set', supported by organisational measures and relatively straightforward technologies such as encryption and access control is preferable [149]. In this view, PbD requires using a DPIA to clarify privacy goals, implement data-minimising mechanisms and identify security controls needed to support the whole [150]. As pointed out by [50], GDPR does not specify how much or of what type of security a system must have, only that it is 'appropriate' and the organisation can demonstrate to the SA that privacy was considered from the start of a project. It is anticipated that adoption of this requirement will rely on further guidance from the ICO and/or WP29.

If this discussion implies controllers will be left confused regarding what they must do to comply with this requirement, the Regulation does offer some relief. Art.25(3) states: "[a]n approved certification mechanism…may be used as an element to demonstrate compliance with the requirements." In fact, GDPR places significant importance on certifications and codes of conduct. They can be used to demonstrate compliance with several aspects of the Regulation including, when combined with enforceable contractual commitments, the legitimisation of data transfer outside the EU [66]. Art.42 encourages SAs at the national and EU level to establish a system of data protection certifications, seals and marks to demonstrate compliance. Rec.99 notes that such schemes would allow data subjects to assess the level of protection offered by products and services. Thus, certification to a recognised standard could act as a powerful market differentiator as well as offering possible mitigation against enforcement actions. It is not yet clear whether this will result in the development of a new series of mandatory standards or whether existing certifications - e.g. ISO/IEC 27001 - will suffice. WP29 will issue guidance on certifications in late 2017 [49].

5.6 Enhanced Data Subject Rights

GDPR affords enhanced rights to data subjects with regards to the collection and processing of their data. Some of these are transposed from existing legislation while others are expanded or entirely new. This Section discusses those new or expanded rights deemed to be most significant: the rights to be informed, erasure, access and data portability.

5.6.1 The Right to be Informed

The right to be informed encompasses the lawfulness, fairness and transparency principle [Art.5(1a)] and, put simply, obligates organisations to tell data subjects that their personal information is being collected, how it will be handled and their rights in respect to their data. This is broadly in line with the second principle of DPA98 and has traditionally been achieved by means of a privacy policy.

A strong argument can be made that the vagueness of the existing rules has resulted, almost inevitably, in the widespread adoption of privacy policies of such Byzantine complexity that most users do not read them. A 2016 study[7] [151] found the average privacy policy is 2,400 words in length and in most cases (78%) permitted third-party sharing of personal data. The same study found only around 1-in-5 users click links to privacy policies and those that do spend little time reading them. This supports a European survey that reported only 18% of respondents fully read privacy statements when registering for a service [59].

Under GDPR, privacy policies will continue to be the main instrument for informing data subjects, however, organisations can no longer present overly complex or verbose statements. Instead, policies must be presented in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" [Art.12(1)]. Subjects must be "made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights" [Rec.39].

The information that must be provided is quite extensive and varies according to whether personal data is being obtained directly from the subject (e.g. filling out a web form) or from another source (e.g. a credit reference agency). There is little value in presenting the required information in this report as it is specified in detail in Arts.12-14. Rather, organisations must simply ensure that their privacy policies are of a sufficient standard. Of course, the terms 'concise', 'transparent' and 'easily accessible' are all subjective and may be difficult to achieve given the expanded list of information that must be specified [152]. Organisations should review their existing policies and how they communicate privacy information to customers. This may include redesigning websites to ensure policies are easily accessible. The content should also be revised to remove or adapt legalistic and technical terms where possible and, crucially, organisations must begin recording how and when notice is given [153]. This is required under the accountability principle and failure to adhere to the required standard may render invalid the data subject's consent, issues that can lead to lower and higher tier penalties respectively.

[7] Examining the privacy policies of the world's top 45 English-language websites.

5.6.2 The Right of Erasure

GDPR gives data subjects the right "[t]o obtain from the controller the erasure of personal data concerning him or her without undue delay" [Art.17(1)] where certain conditions are met. The right to erasure (or right to be forgotten) has raised much interest in the media. It is considerably stronger than its equivalent under the DPA98 which allows erasure only where the data is inaccurate [DPA98, p.10] or likely to cause unwarranted and substantial damage or distress [DPA, p.8]. It is not an unlimited right, however, and individuals may only request erasure where there is no compelling reason for continued processing [ICO, 2017]. One of the following conditions must be met [Art.17(1)].

- The data is no longer necessary for the purpose it was originally collected.
- The subject withdraws their consent and there are no other legal grounds for processing.
- The subject objects to the processing and there are no other legitimate grounds for it to continue, e.g. direct marketing.
- The data has been unlawfully processed, i.e. otherwise in breach of the Regulation.
- The data must be erased to comply with a legal obligation.
- The data relates to offering information society services to a child.

Controllers may refuse an erasure request only where the processing is necessary [Art.17(3)]:

- in exercising the right of freedom of expression;
- to comply with a legal obligation, a task in the public interest or exercise of official authority;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, e.g. scientific, historical or statistical research; or
- the exercise or defence of legal claims.

Clearly the conditions under which a controller can refuse are more limited than those under which a data subject may make a request. Where a controller refuses to comply the burden of proof will be on the organisation to demonstrate that their grounds for refusal override the interests of the data subject. If an organisation is relying on consent to collect and process data, the subject's right to erasure is likely to outweigh the organisation's right to retain it [84]. Thus, controllers must carefully consider their legitimate reasons for holding personal data and be prepared to deal with such requests which could carry significant administrative burden [154].

Time will also be a factor: controllers must act on subject requests within one month, extensible by two further months for complex requests [Art.12(3)]. The same timeframe applies to requests made under the other subject rights. The situation becomes more complicated if the controller has made public or otherwise shared the personal data with third parties. The controller must inform those other parties of the erasure request unless they can demonstrate that doing so would be impossible or involve disproportionate effort [Art.17(2)].

Finally, organisation should consider the issue of shadow IT. This could include employees processing data on personal devices (BYOD) or using services not managed or controlled by the organisation, e.g. cloud-based storage or webmail. The Regulation offers no advice, and certainly no exemptions, for how erasure requests might be handled in such circumstances. Indeed, shadow IT is relevant to all aspects of the Regulation and likely to become a major issue in GDPR compliance [44]. Many information security practitioners will have experience in preventing the compromise of business data in shadow IT so this is another area in which they can add value in supporting compliance. As with the accountability principle, information governance - knowing exactly what information is held and where it is stored - will be key to organisation's ability to comply [64].

5.6.3 The Rights of Access and Data Portability

DPA98 affords data subjects the right to obtain from controllers confirmation that their personal data is being processed and, if so, access to a physical or electronic copy and the purposes of processing, the categories of data being processed and any third parties that have or will receive the data [DPA, p.6]. These are called Subject Access Requests (SARs). Under GDPR this right is largely unchanged and includes only minor additions, e.g. the expected retention period or criteria used to determine the period [Art.15(1)]. SARs can consume significant resource: fewer than 14% of companies can complete one in less than three hours and 43% think they could take longer than a week [12]. To help offset the cost, organisations may currently charge a fee of up to £10 per request, however, GDPR requires that a subject's first SAR be serviced free of charge [Art.15(3)]. This has two practical consequences. The first is the obvious, albeit small, increase in the cost of servicing each request. Potentially more troublesome is that removal of the fee may encourage many more people to submit SARs than do so currently, thus increasing the cost and administrative burden on business. Organisations should prepare to respond to any increase, however, SARs are not a new requirement and those already compliant with DPA98 should face no new difficulties on a technical level. The right of access is closely related to a new right - that of data portability - which has the potential to cause greater difficulties.

GDPR aims to increase individuals' control over their data and encourage competition in the digital economy by making it easier to switch from one service provider to another [107]. It confers on data subjects "the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance…where technically feasible" [Art.20(1-2)]. Thus, the right of data portability is comprised of two components: the first compliments the right of access and specifies that data can be obtained in a structured, commonly used format and the second allows subjects to transfer their data to another controller.

The right to portability is not unlimited. It applies only where processing is automated (i.e. most paper files are excluded) and based on the subject's consent or fulfilment of a contract with the subject [Art.20(1)]. The question of exactly what data is in scope has caused some confusion, for example [155] suggests it applies to only "those data which the data subject…provided directly to a controller" [155. p.232]. There is a danger this may be interpreted as information the subject actively or consciously

gives to the controller, e.g. name, address, age submitted via an online form. This is incorrect. The term 'provided by' should be interpreted broadly to include data observed from the subject's activities such as location information, IoT device usage statistics, search history, activity logs or past purchases. Data created by the controller that is inferred or derived from data provided by the subject in not in scope. Thus, a list of customer purchases from an online store would qualify but a profile created by the controller *based* on their purchases - e.g. to suggest further products - would not [156].

A potential issue is that there is no universal standard that could be used to transfer a potentially wide range of data types [107, 136]. This should not be viewed as a significant obstacle, however, as direct transfers between controllers are only required where 'technically feasible'. GDPR does not create an obligation for controllers to use systems that are compatible but does encourage the development of formats that allow interoperability [Rec.68]. This is defined as: "[t]he capability to communicate…or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units" [157]. WP29 suggests that trade associations and industry stakeholders cooperate to develop standard formats to deliver the right of data portability. This already exists in some sectors, e.g. the ability to transfer banking services from one provider to another. Where there is no agreed standard, personal data should be provided at a high level of abstraction from any proprietary format and in open formats such as XML, CSV and JSON [156].

Organisations should not wait until they receive requests to plan their response: they are subject to the same time limits as discussed in section 5.6.2. Moreover, a controller who do not respond or refuses a request can be reported to the SA and may face an administrative penalty or judicial enforcement to comply [Art.12]. A 2016 survey[8] [9] found 13% of UK adults have submitted SARs. If a similar proportion were to submit portability requests it could represent a significant administrative burden. Organisations for whom automated data processing is a core business activity should identify over which data the right is exercisable and decide in advance what format will be used to transfer it. They should also consider implementing automated means to facilitate exchanges to lessen the burden of numerous or repetitive requests [155, 156]. Although data portability has the potential to require changes in how organisations deal with some types of personal data, [116] observes that it also presents an opportunity to attract new customers by potentially removing some of the existing barriers to switching from between services.

5.7 Summary

This section discussed several of the key challenges GDPR presents to organisations. Though not exhaustive, it served to highlight the relationship between information security and data protection and where the two functions can collaborate to support compliance and improve information governance. Key tasks, such as ensuring that consent is properly obtained and recorded, that organisations understand the requirements of the accountability principle and rights afforded to data subjects were also discussed.

[8] 1,249 members of the public.

PART 6: PROJECT CONCLUSIONS

The aim of this project was to identify the key impacts of GDPR for UK industry. Understanding the implications of GDPR is of significant value to organisations dealing with personal data which, as per section 5.4, represents a majority of British businesses. Adoption of new technologies and the newly expanded definitions of personal data and processing mean this figure is only likely to increase.

This report presented a systematic comparison and synthesis of the differences between the existing law and GDPR to identify those changes judged to represent the greatest practical challenge. It was argued that these comprise of those changes relating to consent, accountability, security and the expansion of data subjects' rights. Each was presented, elaborated and approaches to its application discussed. Perhaps the most significant challenge is the introduction of an accountability principle, meaning it is no longer sufficient for organisations to merely comply with the Regulation: they must keep a record of how they comply and be prepared to evidence this to the ICO. Organisations will need to review their strategies, processes and procedures for handling personal data. They must also demonstrate that privacy has been considered from the outset when developing new products and services, e.g. data minimisation and privacy-friendly default settings.

Comprehensive data audits will be required to identify how much personal data is held, where it is logically and physically located and who has access to it. We observed in section 5.5.1 that this can be compared with the requirements of PCI-DSS for payment card information. Although not examined in detail, the concept of a 'personal data environment' is an intriguing one. The practicality of such a solution would be a worthwhile and potentially valuable topic for further research. Another area of further work could be to develop certifications or standards against which an organisation's protection of privacy can be measured. This may involve the adaption of existing security certifications such as ISO/IEC 27001 or the creation of entirely new ones and is a stated objective of the Regulation [Art.42].

Also discussed in section 5.3 was GDPR's requirements apropos of the security of personal data and how increasingly common breaches should be handled and reported. It was argued that data protection and information security should not be viewed as discrete entities. They are complimentary and it seems unlikely that an organisation holding any significant quantity of personal data can meet its obligations under GDPR without a strong working relationship between the two. While security experts are well placed to protect an organisation's networks and systems and identify incidents indicating a possible breach, they may not be fully aware of how this relates to privacy laws.

The 72-hour timeframe for reporting a breach begins as soon as it is discovered so organisations must implement an effective internal reporting strategy to inform the DPO while avoiding inefficiencies caused by inundating them with false positives. Importantly, many security experts will base their decisions on an assessment of the risk to the organisation but GDPR is concerned with risk to data subjects themselves. This subtle difference means personnel responsible for data protection must engage with those dealing with security to ensure personal data is properly protected. Similarly, the expertise of security personnel should be an important input to DPIAs apropos of controls and

mitigation of risk. They can also contribute to the issue of managing personal data in shadow IT as this is similar to the challenge of protecting corporate information assets in distributed or BYOD environments. GDPR represents an ideal opportunity to drive this convergence. It is hoped the rethinking of security required by GDPR will drive greater adoption of encryption within organisations that do not currently use it, improving the security of all data, not just that falling under the remit of the Regulation.

New rights afforded to data subjects could represent a significant administrative burden, especially if a public increasingly aware of data breaches chooses to exercise those rights more frequently. Many organisations will already have an effective system for dealing with SARs but the new rights of erasure and data portability may cause more difficulty. At the heart of this challenge is, again, understanding what data is being held, how it is processed and stored and with whom it has been shared. The data audits needed to service these requests will require a great deal of preparatory work but will also result in improved data governance and reduction of unnecessary redundancy. As such, they represent an opportunity for increased efficiency and cost savings. Adoption of interoperable systems and data formats will further increase efficiency and allow organisations to benefit by making privacy a market differentiator.

At the time of writing only nine months remain until GDPR comes into force and, as noted in section 3.7, the UK's decision to leave the EU will have no effect on its adoption. Contemporaneous announcements continue to indicate that the new DPA will match the requirements of GDPR: organisations will be held to the same standards for UK citizens' personal data as for that of EU residents. For organisations not yet compliant or that have not begun planning for GDPR, this timescale could represent a serious challenge. Substantial amounts of time, planning and financial resource may be required to implement a GDPR-compliant regime. Even organisations already compliant with DPA98 and with effective procedures for handling personal data and responding to subject requests will have to make changes to meet their new obligations. The amount of work required to collect and maintain the extensive documentation required by the accountability principle, for example, should not be underestimated. The Regulation will be fully enforceable from the outset and organisations that fail to take it seriously could find themselves in breach from day one. Indeed, as discussed in section 1.2, it seems likely that many organisations will not be 100% compliant by May 2018.

Much has been written about the GDPR's substantially increased fines, however, it is worth remembering that the ICO has never invoked its current maximum penalty of £500,000, even in egregious cases [110]. While the scale of potential fines represents a risk no company can afford to ignore, they should not be the primary motivator for data protection reform. Administrative fines are only one tool and the Information Commissioner has debunked speculation about their indiscriminate application: "it is scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm" [158]. Rather, the ICO will use fines as a last resort and take into account genuine efforts an organisation has made towards adopting best practice.

In researching this project it was apparent that there exists a great deal of uncertainty surrounding some aspects of GDPR. This is not helped by sometimes ambiguous terminology, e.g. the lack of distinction between 'risk' and 'high-risk' and how 'explicit consent' differs from mere 'consent'. These may seem simple matters of semantics but, ultimately, the result of many a legal case is determined by how such terms are interpreted. Much of the freely available reference material is outdated, incorrect or at least incomplete. A cynical observer might also note that much freely available material is produced by consultancy firms who may have a vested interest in making GDPR-compliance appear more onerous than it truly is. It is hoped that the next 12 months will see greater scrutiny of GDPR's requirements. Along with further guidance from reputable sources such as the ICO and WP29, this will promote greater clarity and stimulate further academic debate over how data protection and security can work together to benefit organisations while protecting individual rights.

Although GDPR introduces new challenges, this report has demonstrated that the principles underlying the Regulation are, in many ways, little different to those first proposed more than forty years ago. It is evolutionary, not revolutionary in nature and organisations already compliant with DPA98, and that view data protection more than merely a function of compliance, are already well placed to deal with and benefit from it. As with developing a security culture, support for data protection reform must come from the top of organisations. Certain aspects of the Regulation point towards a more business-friendly approach: the introduction of the one-stop-shop for notification of processing means organisations operating internationally will no longer have to approach the SA of each member state individually. Harmonisation of legislation across the EU will also offer increased confidence for those organisations. In the words of one commentator: "GDPR doesn't have to be GDP-Argh!" [159].

BIBLIOGRAPHY

[1] European Parliament (2016). *Regulation (EU) 2016/679/EC 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)*. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [Accessed 14 Jan 2017].

[2] European Parliament (1995). *Directive 95/46/EC (EU) on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [Accessed 14 Jan 2017].

[3] United Kingdom (1998). *Data Protection Act 1998*. Available at: http://www.legislation .gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf [Accessed 14 Jan 2017].

[4] Denham, E. (2016). *How the ICO Will be Supporting the Implementation of the GDPR*, ICO Blog. Available at: https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/ [Accessed 23 Feb 2017].

[5] Prime Minister's Office (2017). *The Queen's Speech and Associated Background Briefing, on the Occasion of the Opening of Parliament on Wednesday 21 June 2017*. Available at: https:// www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech _2017_background_notes.pdf [Accessed 17 Jul 2017].

[6] Reding, V. (2011). The upcoming data protection reform for the European Union, *International Data Privacy Law*, 1(1), pp.3-5. Available at: https://academic.oup.com [Accessed 1 Aug 2017].

[7] Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten, *Computer Law & Security Review*, 29(3), pp.229-235. Available at: https://ssrn.com/abstract=2473151 [Accessed 8 Jul 2017].

[8] Department for Culture, Media & Sport (2017). *Cyber Security Breaches Survey 2017*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/ Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf [Accessed 4 Aug 2017].

[9] Information Commissioner's Office (2016). *Annual Track Survey*. Available at: https://ico.org.uk /about-the-ico/our-information/research-and-reports/information-rights-research/ [Accessed 8 Aug 2017].

[10] PricewaterhouseCoopers (2017). *Number of fines for UK data privacy issues doubles and totals £3.2m*, PwC UK. Available at: https://www.pwc.co.uk/press-room/press-releases/number-of-fines-for-UK-data-privacy-issues-doubles.html [Accessed: 15 Aug 2017].

[11] Shred-it (2017). *Security Tracker 2017*. Available at: https://www.shredit.co.uk/en-gb/about/ press-room/press-releases/more-than-half-of-uk-business-owners-unaware-of-in [Accessed 18 Jul 2017].

[12] Exonar (2017). *UK GDPR Preparedness Survey*. Available at: https://www.exonar.com/2017 /07/31/uk-gdpr-preparedness-survey/ [Accessed 9 Aug 2017].

[13] Kempner, R. (1946). The German National Registration System as Means of Police Control of Population, *Journal of Criminal Law and Criminology (1931-1951)*, 36(5), pp.362-387. Available at: http://www.jstor.org/stable/1138058 [Accessed 10 Feb 2017].

[14] Black, E. (2001). *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. London: Random House.

[15] Heide, L. (2009). *Punched-card systems and the early information explosion, 1880–1945*. Baltimore: John Hopkins University Press.

[16] Aly, G. and Roth, K (2004). *The Nazi Census: Identification and Control in the Third Reich*. Philadelphia: Temple University Press.

[17] Shaw, T. (2013). *Privacy Law and History: WWII Forward*, International Association of Privacy Professionals. Available at: https://iapp.org/news/a/2013-03-01-privacy-law-and-history-wwii-forward/ [Accessed 3 Jun 2017].

[18] Vlemmix, P (2012). *Panopticon* [video]. Available at: https://www.youtube.com/watch ?v=FUyB0Tsj6jE [Accessed 25 Jul 2017].

[19] McCartey-Snead, S. and Hilby, A (2013). Research Guide to European Data Protection Law, *Legal Research Series,* University of California, Berkeley School of Law. Available at: http:// demo.berkeleylaw.bepress.com/leg_res/1/ [Accessed 5 Feb 2017].

[20] Kotzker, J. (2002). The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad, *St. Thomas Law Review*, vol. 15, pp.727-756. Available at: http://heinonline.org [Accessed 11 Jun 2017].

[21] United Nations General Assembly (1948). *The Universal Declaration of Human Rights (217 [III] A)*. Available at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf [Accessed 10 Feb 2017].

[22] Council of Europe (1950), *European Convention for the Protection of Human Rights and Fundamental Freedoms*. Available at: http://www.echr.coe.int/Documents/Convention_ENG .pdf [Accessed 10 Feb 2017].

[23] Council of Europe (2017). *Do Not Get Confused*, The Council of Europe in Brief. Available at: http://www.coe.int/en/web/about-us/do-not-get-confused [Accessed 11 Jun 2017].

[24] Council of Europe (2017), *Convention 108 and Protocol: Background*. Available at: http://www .coe.int/en/web/data%20-protection/background [Accessed 1 Aug 2017].

[25] Carey, P (2009). *Data Protection: A Practical Guide to UK and EU Law*, 3rd ed. New York: Oxford University Press.

[26] Murray, A. (2016). *Information Technology Law*, 3rd ed. Oxford: Oxford University Press.

[27] Younger, K. (1972). *Report of the Committee on Privacy*, Cmnd 5012. London: HMSO.

[28] Lindop, N. (1978). *Report of the Committee on Data Protection*, Cmnd 7341. London: HMSO.

[29] Critchell-Ward, A. and Landsborough-McDonald, K. (2007). Data protection law in the European Union and the United Kingdom. *Comparative Law Yearbook of International Business*, vol. 29, pp.515-578. London: Kluwer Law International.

[30] Rowland, D., Kohl, U. and Charlesworth, A. (2011). *Information Technology Law*, 4th ed. London: Routledge.

[31] Home Office (1975). *White Paper on Computers and Privacy*, Cmnd 6353. London: HMSO.

[32] Warren, A. and Dearnley, J. (2005). Data protection legislation in the United Kingdom. *Information, Communication & Society*, 8(2), pp.238-263. Available at: http://www .tandfonline.com/doi/abs/10.1080/13691180500146383 [Accessed 2 Feb 2017].

[33] Lloyd, I. (2014). *Information Technology Law*, 7th ed. Oxford: Oxford University Press.

[34] Council of Europe (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 [Accessed 10 Feb 2017].

[35] Home Office (1982). *White Paper on Data Protection: The Government's Proposal for Legislation*, Cmnd 8539. London: HMSO.

[36] United Kingdom (1984). *Data Protection Act 1984*. Available at: http://www.legislation .gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf [Accessed: 14 Jan 2017].

[37] Room, S. (2009). *Butterworth's Data Security: Law & Practice*. London: LexisNexis.

[38] Reed, C. (2012). *Making laws for cyberspace*. Oxford: Oxford University Press.

[39] Bainbridge, D. (2008). *Introduction to Information Technology Law*. Harlow: Pearson Longman.

[40] Information Commissioner's Office (2017). *Data Protection Principles*. Available at: https:// ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ [Accessed 5 Jun 2017].

[41] Information Commissioner's Office (2017). *The Rights of Individuals (Principle 6)*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/ [Accessed 15 Jul 2017].

[42] European Commission (2017). *Commission decisions on the adequacy of the protection of personal data in third countries*. Available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm [Accessed 11 Jun 2017].

[43] Court of Justice of the European Union (2015). *Judgement of the Court (Grand Chamber) of 6 October 2015 (ECLI:EU:C:2015:650) Maximillian Schrems v. Data Protection Commissioner*. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&page Index=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=162892 [Accessed 11 Jun 2017].

[44] Krystlik, J. (2017). With GDPR, preparation is everything, *Computer Fraud & Security*, 2017(6), pp.5-8. Available at: http://www.sciencedirect.com [Accessed 25 Jul 2017].

[45] Goldstein, D., Hardiman, M., Baker, M. and Druckerman, J. (2016). Understanding the EU–US Privacy Shield Data Transfer Framework, *Journal of Internet Law*, 20(5), pp.17-22. Available at: https://www.ebscohost.com [Accessed 11 Jun 2017].

[46] Information Commissioner's Office (2015). *Guidance about the issuing of monetary penalties*. Available at: https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf [Accessed 12 Jun 2017].

[47] Thomson Reuters (2015). *Sanctions for data breaches*. Available at: https://uk.practicallaw .thomsonreuters.com/5-518-8056?originationContext=knowHow&transitionType=KnowHow Item&contextData=(sc.DocLink)&firstPage=true&bhcp=1 [Accessed 12 Jun 2017].

[48] European Commission (2016). *Article 29 Working Party*. Available at: http://ec.europa.eu /newsroom/just/item-detail.cfm?item_id=50083 [Accessed 11 Jun 2017].

[49] Article 29 Working Party (2016). *Work Programme 2016 – 2018*. Available at: http://ec.europa .eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp235 _en.pdf [Accessed 11 Jun 2017].

[50] Calder, A. (2016). *EU GDPR: A Pocket Guide*. Cambridge: IT Governance Publishing.

[51] Internet World Stats (2017). *Internet Growth Statistics 1995 to 2017*. Available at: http://www .internetworldstats.com/emarketing.htm [Accessed 12 Jun 2017].

[52] European Commission (2012). *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (IP/12/46)*. Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en [Accessed 12 Jun 2017].

[53] Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance, *Network Security*, 2017(6), pp.8-11. Available at: http://www.sciencedirect.com [Accessed 25 Jul 2017].

[54] European Commission (2010). *European Commission sets out strengthen EU data protection rules (IP/10/1462)*. Available at: http://europa.eu/rapid/press-release_IP-10-1462_en.htm ?locale=en [Accessed 12 Jun 2017].

[55] Grest, L. and Ryz, L. (2016). A new era in data protection. *Computer Fraud & Security*, 2016(3), pp.18-20. Available at: www.sciencedirect.com [Accessed 11 Feb 2017].

[56] Jay, R. (2017). Background. In Jay, R. (ed.), *Guide to the General Data Protection Regulation*. pp.1-14. London: Sweet & Maxwell.

[57] European Commission (2015). *A Digital Single Market Strategy for Europe (COM (2015) 192)*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri= CELEX%3A52015DC0192 [Accessed 12 Jun 2017].

[58] European Commission (2015). *Agreement on Commission's EU data protection reform will boost Digital Single Market*. Available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm [Accessed 18 Jul 2017].

[59] European Commission (2015). *Special Eurobarometer 431 on Data Protection*. Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_ eurobarometer_240615_en.pdf [Accessed 12 Jun 2017].

[60] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 6(2), pp.77-78. Available at: https://academic-oup-com [Accessed 11 Feb 2017].

[61] CJEU (2016). *Judgement of the Court (Second Chamber) 19 October 2016 (C-582/14) Patrick Brayer v. Bundesrepublik Deutschland*. Available at: http://curia.europa.eu/juris/document/ document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&p art=1&cid=1116945 [Accessed 13 Jun 2017].

[62] De Silva, S. and Liu, A. (2017). Europe's tough new law on biometrics, *Biometric Technology Today*, 2017(2), pp.5-7. Available at: http://www.sciencedirect.com [Accessed 25 Jul 2017].

[63] HSBC (2017). *Voice ID*, HSBC UK. Available at: https://www.hsbc.co.uk/1/2/contact-and-support/banking-made-easy/voice-id [Accessed 13 Jun 2017].

[64] Tankard, C. (2016). What the GDPR means for businesses, *Network Security*, 2016(6), pp.5-8. Available at: https://www.sciencedirect.com [Accessed 11 Feb 2017].

[65] Hillen, C., Hoepman, J. and Colesky, M. (2016). A Critical Analysis of Privacy Design Strategies, *Proceedings of the IEEE*, pp.33-40. Available at: ieeexplore.ieee.org [Accessed 20 Feb 2017].

[66] Gilbert, F. (2016). EU General Data Protection Regulation: What Impact for Businesses Established Outside the European Union?, *Journal of Internet Law*, 19(11), pp.3-8. Available at: http://web.b.ebscohost.com [Accessed 14 Feb 2017].

[67] Mansfield-Devine, S. (2016). Data Protection: Prepare Now or Risk Disaster, *Computer Fraud & Security*, 2016(12), pp.5-12. Available at: https://www.sciencedirect.com [Accessed 14 Feb 2017].

[68] Veritas Technologies LLC (2017). *2017 Veritas GDPR Report*. Available at: https://www.veritas .com/content/dam/Veritas/docs/reports/gdpr-report-en.pdf [Accessed 18 Jul 2017].

[69] Ismail, N. (2017). *Majority of CISO's Begin Prioritising GDPR Compliance*, Information Age. Available at: http://www.information-age.com/cisos-begin-prioritising-gdpr-compliance-123466282/ [Accessed 18 Jul 2017].

[70] Webroot (2017). *Ready or Not: SMBs and the GDPR*. Available at: https://s3-us-west-1.amazonaws.com/webroot-cms-cdn/3414/9799/1847/Webroot_GDPR_Report.pdf [Accessed 17 Jul 2017].

[71] Marr, B. (2017). *What every small business must know about GDPR*, Hiscox Business Blog. Available at: https://www.hiscox.co.uk/business-blog/every-small-business-must-know-gdpr-new-data-privacy-law/ [Accessed 18 Jul 2017].

[72] Lobel, B. (2017). *What does GDPR mean to me and my business?,* Small Business. Available at: http://smallbusiness.co.uk/dealing-with-cyber-attacks-2538554/ [Accessed 18 Jul 2017].

[73] Dunn, J. (2016). *Brexit and the GDPR - why leaving the EU will make life harder for enterprise*, Computerworld UK. Available at: http://www.computerworlduk.com/security/brexit-gdpr-why-leaving-eu-will-make-life-harder-for-enterprises-3641825/ [Accessed 18 Jul 2017].

[74] McDowell, C. (2017). *GDPR: The Risks to SMEs and Those Who Insure Them*. Available at: https://doorda.com/lugus/smes-exposure-gdpr/ [Accessed 18 Jul 2017].

[75] Bergamo, L. (2016). *Get Ready for General Data Protection Regulation (GDPR).* Available at: https://www.actiance.com/blog/get-ready-gdpr/ [Accessed 18 Jul 2017].

[76] Wheeler, B. (2017). *GDPR: Do you really need a Data Protection Officer (DPO)*. Available at: http://www.ascentor.co.uk/2017/06/gdpr-data-protection-officer-dpo/ [Accessed 18 Jul 2017].

[77] Brown, P. (2017). *EU GDPR Special Focus* [presentation], Infosecurity Europe 2017, 7 Jun 2017, London.

[78] BBC (2017). *Article 50: Theresa May to trigger Brexit process next week*, BBC News. Available at: http://www.bbc.co.uk/news/uk-politics-39325561 [Accessed 17 Jul 2017].

[79] Kefron (2016). *Brexit & GDPR: How Will UK Businesses Be Affected?* Available at: https://www.kefron.com/blog/brexit-gdpr-will-uk-businesses-affected/ [Accessed 17 Jul 2017].

[80] Metzger, M. (2016). *UK Businesses Confused over GDPR and Brexit*, SC Magazine UK. Available at: https://www.scmagazineuk.com/uk-businesses-confused-over-gdpr-and-brexit/article/568304/ [Accessed 17 Jul 2017].

[81] Gough, O. (2017). *SMEs uncertain of Brexit impact on GDPR*, Small Business. Available at: http://smallbusiness.co.uk/smes-uncertain-brexit-impact-gdpr-2539200/ [Accessed 17 Jul 2017].

[82] Denham, E. (2016). *How the ICO Will be Supporting the Implementation of the GDPR*, ICO Blog. Available at: https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/ [Accessed 23 Feb 2017].

[83] Department for Culture, Media & Sport (2017). *Call for Views on the General Data Protection Regulation Derogations*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/610133/EnglishGDPRCFV_v1.5.2pdf_2.pdf [Accessed 17 Jul 2017].

[84] Beckett, P. (2017). GDPR compliance: your tech department's next big opportunity, *Computer Fraud & Security*, 2017(5), pp.9-13. Available at: http://www.sciencedirect.com [Accessed 25 Jul 2017].

[85] Linkomies, L. (2017). Brexit Hampers SME Firms' GDPR Preparations, *Privacy Laws & Business*, no. 91, p.2. Available at: http://www.privacylaws.com/Documents/PLB_UK_SPL/uknews91.pdf [Accessed 17 Jul 2017].

[86] Rossi, B. (2017). *1 in 4 UK Businesses Have Cancelled Preparations for GDPR*, Information Age. Available at: http://www.information-age.com/1-4-uk-businesses-cancelled-preparations-gdpr-123465421/ [Accessed 17 Jul 2017].

[87] Metzger, M. (2017). *Brexit Bust Bamboozles GDPR Preparation for British Business*, SC Magazine UK. Available at: https://www.scmagazineuk.com/brexit-bust-bamboozles-gdpr-preparation-for-british-business/article/651133/ [Accessed 17 Jul 2017].

[88] Gardner, S. (2016). *Brexit May Undercut Privacy Compliance: U.K. Official*, Bloomberg BNA. Available at: https://www.bna.com/brexit-may-undercut-n57982079026/ [Accessed 17 Jul 2017].

[89] United Kingdom (2017). *European Union (Withdrawal) Bill 2017-19 [HC 5]*. Available at: http://services.parliament.uk/bills/2017-19/europeanunionwithdrawal.html [Accessed: 17 Jul 2017].

[90] BBC (2017). *Queen's Speech: New Data Protection Law*, BBC News. Available at: http://www.bbc.co.uk/news/technology-40353424 [Accessed 17 Jul 2017].

[91] Donn, P. (2017). *The UK's New Data Protection Bill and the GDPR go Hand in Hand*, Data Protection Network. Available at: https://www.dpnetwork.org.uk/opinion/uk-data-protection-bill-gdpr/ [Accessed 17 Jul 2017].

[92] Mason, R. (2017). *UK citizens to get more rights over personal data under new laws*, The Guardian. Available at: https://www.theguardian.com/technology/2017/aug/07/uk-citizens-to-get-more-rights-over-personal-data-under-new-laws [Accessed 15 Aug 2017].

[93] European Commission (2017). *Data Transfers Outside the EU*. Available at: http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm [Accessed 17 Jul 2017].

[94] Woodhouse, J. (2017). Brexit and Data Protection, *House of Commons Library Briefing Papers,* no. 7838. Available at: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-7838 [Accessed 17 Jul 2017].

[95] House of Lords Select Committee on the European Union (2017). *Corrected Oral Evidence: The EU Data Protection Package (01 March 2017)*. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48742.pdf [Accessed 17 Jul 2017].

[96] House of Lords Select Committee on the European Union (2017). *Corrected Oral Evidence: The EU Data Protection Package (08 March 2017)*. Available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.pdf [Accessed 17 Jul 2017].

[97] Lashmar, P. (2016). *Snoopers' Charter: why journalists (and the rest of us) should be afraid*, The Conversation. Available at: http://theconversation.com/snoopers-charter-why-journalists-and-the-rest-of-us-should-be-afraid-69591 [Accessed 18 May 2017].

[98] MacAskill, E. (2016). *'Extreme surveillance' becomes UK law with barely a whimper*, The Guardian. Available at: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper [Accessed 18 Apr 2017].

[99] Bernal, P. (2016). *How the UK passed the most invasive surveillance law in democratic history*, The Conversation. Available at: http://theconversation.com/how-the-uk-passed-the-most-invasive-surveillance-law-in-democratic-history-69247 [Accessed 18 May 2017].

[100] Fiveash, K. (2017). *UK forced to derail Snoopers' Charter blanket data slurp after EU ruling*, Ars Technica UK. Available at: https://arstechnica.co.uk/tech-policy/2017/02/investigatory-powers-law-missing-draft-communications-data-code/ [Accessed 18 Jul 2017].

[101] Bowcott, O. (2016). *EU's highest court delivers blow to UK snooper's charter*, The Guardian. Available at: https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter [Accessed 18 Jul 2017].

[102] CJEU (2016). *Judgement of the Court (Grand Chamber) of 21 December 2016 (ECLI:EU:C:2016:970) Joined Cases C-203/15 and C-698/15 (Home Office v. Watson)*. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=515948 [Accessed 18 Jul 2017].

[103] Maldoff, G. (2016). *Top 10 Operational Impacts of the GDPR: Part 3 – Consent*, International Association of Privacy Professionals. Available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/ [Accessed 20 Feb 2017].

[104] Information Commissioner's Office (2014). *Conducting Privacy Impact Assessments Code of Practice*. Available at: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf [Accessed 22 Feb 2017].

[105] Wolters, P. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility?, *International Data Privacy Law*, pp.1-14. Available at: https://academic.oup.com [Accessed 3 Jun 2017].

[106] Jay, R. and Townsend, L. (2017). Security Obligations and Breach Notification. In Jay, R. (ed.), *Guide to the General Data Protection Regulation*, pp.131-141. London: Sweet & Maxwell.

[107] Long, I. (2016). *Data Protection: The New Rules*. Bristol: Jordan.

[108] Information Commissioner's Office (2012). *Notification of data security breaches to the Information Commissioner's Office (ICO)*. Available at: https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf [Accessed 25 Jul 2017].

[109] ESET (2017). *Is GDPR Good or Bad News for Business?* Available at: http://www.welivesecurity.com/wp-content/uploads/2017/02/Is-GDPR-good-or-bad-news-for-business.pdf [Accessed 22 Feb 2017].

[110] Information Commissioner's Office (2016). *TalkTalk gets record £400, 000 fine for failing to prevent October 2015 attack*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/ [Accessed 24 Feb 2017].

[111] Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Officers ('DPOs')*. Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [Accessed 5 Aug 2017].

[112] Information Commissioner's Office (2017). *Consultation: GDPR consent guidance*. Available at: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf [Accessed 14 Aug 2017].

[113] Titcomb, J. (2015). *Britain opts out of EU law setting social media age of consent at 16*, The Telegraph. Available at: http://www.telegraph.co.uk/technology/internet/12053858/Britain-opts-out-of-EU-law-raising-social-media-age-of-consent-to-16.html [Accessed 24 Feb 2017].

[114] International Organisation for Standardisation (2014). *ISO/IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary*.

[115] Committee on National Security Systems (2015). *Committee on National Security Systems (CNSS) Glossary*. CNSS Instruction No. 4009. Available at: https://www.cnss.gov/CNSS/openDoc.cfm?+ghcEhZHViSkZkpmkCUbPQ== [Accessed 2 Aug 2017].

[116] Calder, A., Campo, R. and Ross, A. (2016). *EU General Data Protection Regulation (GDPR): an implementation and compliance guide*. Cambridge: IT Governance Publishing.

[117] Calder, A. and Watkins, S. (2015). *IT Governance: an international guide to data security and ISO27001/ISO27002*, 6th ed. London: Kogan Page.

[118] Green, A. (2017). Ransomware and the GDPR, *Network Security*, 2017(3), pp.18-19. Available at: http://www.sciencedirect.com [Accessed 25 Jul 2017].

[119] Saltzer, J. and Schroeder, M. (1975). The protection of information in computer systems, *Proceedings of the IEEE*, 63(9), pp.1278-1308. Available at: http://ieeexplore.ieee.org/ [Accessed 3 Aug 2017].

[120] Dunn, J. (2017). *22 of the Most Infamous Data Breaches*, Techworld. Available at: http://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/ [Accessed 2 Aug 2017].

[121] Masters, G. (2017). *Ransomware attacks will double in 2017*, SC Magazine. Available at: https://www.scmagazine.com/ransomware-attacks-will-double-in-2017-study/article/634560/ [Accessed 2 Aug 2017].

[122] BBC (2017). *NHS cyber-attack: GPs and hospitals hit by ransomware*, BBC News. Available at: http://www.bbc.co.uk/news/health-39899646 [Accessed 2 Aug 2017].

[123] Hall, K. (2017). *NHS Digital stopped short of advising against paying off WannaCrypt*, The Register. Available at: https://www.theregister.co.uk/2017/05/25/nhs_digital_did_not_advise_against_paying_wannacrypt/ [Accessed 3 Aug 2017].

[124] ICO (2017). *ICO statement on recent cyber attacks on the NHS*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/ico-statement-on-recent-cyber-attacks-on-the-nhs/ [Accessed 2 Aug 2017].

[125] BBC (2017). *NHS was repeatedly warned of cyber-attack*, BBC News. Available at: http://www.bbc.co.uk/news/uk-39912825 [Accessed 2 Aug 2017].

[126] The Guardian (2017). *Jeremy Hunt 'ignored warning signs' before cyber-attack hit NHS*, The Guardian. Available at: https://www.theguardian.com/society/2017/may/13/jeremy-hunt-ignored-warning-signs-before-cyber-attack-hit-nhs [Accessed 2 Aug 2017].

[127] Rice, S. (2016). *Being held to ransom?,* ICO Blog. Available at: https://iconewsblog.org.uk/2016/12/15/being-held-to-ransom/ [Accessed 2 Aug 2017].

[128] Information Commissioner's Office (2017). *Monetary Penalty Notice - Boomerang Video Ltd*. Available at: https://ico.org.uk/media/action-weve-taken/mpns/2014300/mpn-boomerang-video-ltd.pdf [Accessed 3 Aug 2017].

[129] Information Commissioner's Office (2017). *Monetary Penalty Notice - Gloucester City Council*. Available at: https://ico.org.uk/media/action-weve-taken/mpns/2014217/gloucester-city-council-mpn-20170525.pdf [Accessed 3 Aug 2017].

[130] Information Commissioner's Office (2017). *Monetary Penalty Notice – London Borough of Islington*. Available at: https://ico.org.uk/media/action-weve-taken/mpns/2014671/mpn-london-islington-20170807.pdf [Accessed 19 Aug 2017].

[131] Information Commissioner's Office (2016). *Monetary Penalty Notice - Historical Society*. Available at: https://ico.org.uk/media/action-weve-taken/mpns/1625357/mpn-historical-society-20161107.pdf [Accessed 3 Aug 2017].

[132] Lucas, E. (2017). *Unsafe Harbor – how will today's regulations affect tomorrow's operations?*, Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/teiss17-gdpr-cause-regulatory/ [Accessed 16 Jul 2017].

[133] Heimes, R. (2016). *Top 10 operational impacts of the GDPR: Part 1 – Data Security and Breach Notification*, International Association of Privacy Professionals. Available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/ [Accessed 3 Aug 2017].

[134] Denham, E. (2017). *GDPR and accountability*. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/ [Accessed 16 Feb 2017].

[135] Jay, R. (2017). Accountability. In Jay, R. (ed.), *Guide to the General Data Protection Regulation*, pp.169-191. London: Sweet & Maxwell.

[136] Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2017). EU General Data Protection Regulation: Changes and implications for personal data collecting companies, *Computer Law & Security Review (2017)*. Available at: http://www.sciencedirect.com [Accessed 25 Jul 2017].

[137] Brennecker, P. (2016). *PCI DSS is a Useful Tool in GDPR Compliance*, SRM Solutions. Available at: http://blog.srm-solutions.com/pci-dss-is-a-useful-tool-in-gdpr-compliance/ [Accessed 22 Feb 2017].

[138] Scott, C. (2016). *GDPR Compliance, is PCI-DSS the Answer?*, The Bunker. Available at: http://www.thebunker.net/gdpr-compliance-is-pci-dss-the-answer/ [Accessed 22 Feb 2017].

[139] 24 Solutions (2016). *EU GDPR – Regulating security that should already be in effect*. Available at: https://www.24solutions.com/en/wp-content/uploads/sites/3/2016/07/24S_EU-GDPR_white paper_EN_28072016.pdf [Accessed 22 Feb 2017].

[140] Ataya, G. (2010). PCI-DSS Audit and Compliance, *Information Security Technical Report*, 15(4), pp.138-144. Available at: http://www.sciencedirect.com [Accessed 22 Feb 2017].

[141] House of Commons Justice Committee (2013). *The functions, powers and resources of the Information Commissioner*. Available at: https://www.publications.parliament.uk/pa/cm 201213/cmselect/cmjust/962/962.pdf [Accessed 22 Feb 2017].

[142] Information Commissioner's Office (2017). *Information Commissioner's Annual Report and Financial Statements 2016/17*. Available at: https://ico.org.uk/media/about-the-ico/documents /2014449/ico053-annual-report-201617-s12-aw-web-version.pdf [Accessed 11 Aug 2017].

[143] Article 29 Data Protection Working Party (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high-risk" for the purposes of Regulation 2016/679*. Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [Accessed 5 Aug 2017].

[144] Mahmood, S. and Power, L. (2016). *Getting to Know the General Data Protection Regulation, Part 6 – Designing for Compliance*. Privacy Law Blog. Available at: http://privacylawblog .fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-6-designing-for-compliance/ [Accessed 23 Feb 2017].

[145] Terstegge, J. (2017). *The EU's Privacy by Default 2.0*, International Association of Privacy Professionals. Available at: https://iapp.org/news/a/the-eus-privacy-by-default-2-0/ [Accessed 23 Feb 2017].

[146] Garside, J. (2014). *Facebook bows to pressure on privacy settings for new users*, The Guardian. Available at: https://www.theguardian.com/technology/2014/may/22/facebook-privacy-settings-changes-users [Accessed 27 Jul 2017].

[147] Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Canada: Information and Privacy Commissioner of Ontario. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf [Accessed 23 Feb 2017].

[148] van Rest, J., Boonstra, D., Everts, M., van Rijn, M. and van Paassen, R. (2014). Designing privacy-by-design. In Preneel, B. and Ikonomou, D. (eds.), *Lecture Notes in Computer Science (Privacy Technologies and Policy),* vol. 8319, pp.55-72. Berlin: Springer Available at: http://link.springer.com [Accessed 22 Feb 2017].

[149] Leenes, R. and Koops, B. (2013). Privacy regulation cannot be hardcoded: A critical comment on the 'privacy by design' provision in data-protection law, *International Review of Law, Computers & Technology*, 28(2), pp.159-171. Available at: http://www.tandfonline.com [Accessed 21 Feb 2017].

[150] Spiekermann, S. (2012). The challenges of privacy by design, *Communications of the ACM*, 55(7), p.38. Available at: http://dl.acm.org [Accessed 15 Aug 2017].

[151] Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment, *Computers in Human Behaviour*, no. 55, pp.992-1000. Available at: http://www.sciencedirect.com [Accessed 11 Jun 2017].

[152] Jay, R., Bapat, A. and Townsend, L. (2017). Transparency and Procedural Rules for the Individual Rights. In Jay, R. (ed.), *Guide to the General Data Protection Regulation*. London: Sweet & Maxwell.

[153] Information Commissioner's Office (2016). *Privacy notices, transparency and control: a code of practice on communicating privacy information to individuals*. Available at: https://ico.org.uk /media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf [Accessed 7 Aug 2017].

[154] Mathy, K. (2016). Key Provisions and Implications for Businesses of the New General Data Protection Regulation, *Journal of Intellectual Property Law & Practice*, 11(12), pp.886-888. Available at: https://academic.oup.com/jiplp/article/11/12/886/2612886/Key-provisions-and-implications-for-businesses-of [Accessed 14 Feb 2017].

[155] Parry, E. (2017). Subject Access and Data Portability. In Jay, R. (ed.), *Guide to the General Data Protection Regulation*, p.231-262. London: Sweet & Maxwell.

[156] Article 29 Data Protection Working Party (2017). *Guidelines on the right to data portability*. Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 [Accessed 5 Aug 2017].

[157] International Organisation for Standardisation (2015). *ICO/IEC 2382, Information technology - Vocabulary*. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en [Accessed 8 Aug 2017].

[158] Denham, E. (2017). *GDPR – sorting the fact from the fiction*, ICO Blog. Available at: https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ [Accessed 15 Aug 2017].

[159] Humphries, S. (2017). *GDPR Doesn't Need to be GDP-Argh!,* Dark Reading. Available at: http://www.darkreading.com/endpoint/gdpr-doesnt-need-to-be-gdp-argh!/a/d-id/1328568 [Accessed 11 Aug 2017].