THE EFFECTS OF BREXIT ON GDPR IMPLEMENTATION

An investigation into data protection legislation within the United Kingdom post-Brexit

Master's Thesis

in Archival Studies

Leiden University

By

Alexander van Goethem

2018

Supervisor: Dr. Paul Brood

Word Count: 22,449

TABLE OF CONTENTS

Introduction

Since its approval on April 14th 2016 the Member States of the European Union, and any companies with interests in the European Union, have been preparing for the largest change in European data protection law in two decades; the General Data Protection Regulation, commonly shortened to GDPR. This legislation replaces the longstanding, but now defunct 1995 Data Protection Directive 95/46/EC, which due to the advances and rapid changes in our technological environment since its adoption has seen its laws no longer meeting modern requirements. The GDPR aims to bring the laws up to speed with technology of today by seeking to bring further protection and ownership to individuals and their data, in addition to harmonising data protection and privacy law throughout all 28 Member States of the EU, simplifying the regulatory environment for organisations and business utilising and processing personal data of EU individuals.[1] Its updated principles, which emphasise the protection of individuals' personal data, seek to regain the levels of trust that have been lost over the last decade due to the mistreatment of personal data by large data processors, and exacerbated by the Edward Snowden leaks in 2013 which exposed a number of US surveillance programmes involving the large-scale collection of personal data, pushing individual data protection to the forefront of the public's collective conscience.[2] Low levels of trust were further demonstrated by findings in the 'Data Protection Eurobarometer' 2015 survey which concluded that 63% of respondents do not trust online businesses and 62% did not trust phone companies and internet service providers,[3] only 15% of respondents felt that they had complete control over the information they provided online.[4] The EU wishes to drastically improve these numbers so that consumers increase their trust in data processors and hence increase online business opportunities within the EU digital market.

Technically the GDPR has been in force since its approval in 2016, though May 25 2018 will see it come into full enforcement, including the introduction of extremely heavy fines of up to 20 million euros or 4% of annual global turnover, whichever is highest, for infringement of the provisions set out in the legislation.[5]

The United Kingdom, though planning on leaving the European Union following the decision made by the British referendum on EU membership in June 2016 famously termed 'Brexit', will still be a

[1] Zerlang 2017, 8.
[2] Christou 2017, 180.
[3] European Union 2015, *Special Eurobarometer 'Data Protection*', 7.
[4] European Union 2015, *Special Eurobarometer 'Data Protection*', 6.
[5] European Union 2016, *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* 247.

Member State of the Union on the date that the GDPR comes into full effect, thus the laws, and more importantly, the consequences for potential non-compliance, will apply until the United Kingdom has officially withdrawn from the EU in March 2019. To manage this issue the British Parliament has proposed the introduction of the temporary 'Data Protection Bill 2017-19', which will adopt the GDPR into British law with some alterations.[6] A key aim of this thesis will be to investigate these deviations of the British law from that of the rest of the EU. Taking this into consideration my thesis statement is: 'Whilst the government of the United Kingdom has prepared the 'Data Protection Bill 2017-19' its position as a 'third country' following the enforcement of the GDPR will decrease its data flow with EU Member States, resulting in a long-term weakening of digital business and lessened personal data security for British individuals'.

A historical analysis of laws similar to the GDPR and the evolution of legislation which has led us to this point will begin this thesis, forming a base of information and understanding so that the new legislation, and the reasoning behind its adoption can be fully understood. In doing so, comparable legislation will be analysed from across the world, and the GDPR's predecessor in both the United Kingdom and the Netherlands will be discussed.

The analysis from Chapter 1 will then be incorporated within a discussion of the changes being introduced by the GDPR legislation, accompanied by an analysis of the flaws, if any, of the GDPR and its future as a leading data protection legislation. Chapter 2 will conclude with a discussion of how the GDPR's changes will affect the archive sector specifically.

Expanding upon this investigation Chapter 3 will aim its focus specifically toward the United Kingdom, leading to an in-depth discussion of the GDPR's effects on a country that is momentarily 'within limbo' due to its unclear position in the European Union, as preparations to withdraw EU membership continue. The British government has stated that it wishes to "maintain the unhindered flow of data between the United Kingdom and the EU post Brexit",[7] and the temporary 'Data Protection Bill 2017-19', has been formulated to ensure this during the United Kingdom's transition out of the EU. The new legislation replaces the 'Data Protection Act' of 1998 which previously provided the legal framework for data protection in the United Kingdom. In the analysis of the proposed legislation this chapter will highlight and explain the differences between the British Data Protection Bill and the GDPR, considering what the consequences of these differences could mean to both individuals and businesses within the United Kingdom. This is only a temporary solution however, and once the United Kingdom has officially left the EU in 2019 it will become a 'third

[6] *Data Protection Bill 2017*.
[7] Hancock 2017.

country' according to GDPR law, meaning many laws of the GDPR and 'Data Protection Bill' will no longer apply. Following on from the thesis statement this section of the thesis will thus investigate further the United Kingdom's position as a 'third country', looking at the effects on business and the British digital economy especially in regard to business conducted with Member States of the European Union once the UK has left. The 'future partnership paper' published by the UK government in August 2017 explores this issue by highlighting the possibilities of a UK-EU model for exchanging and protecting personal data post-Brexit, building upon the existing 'Data Protection Bill'.[8]

The final chapter will discuss one of the most important aspects of data protection legislation in Europe; the Data Protection Authorities. Starting this section of the work will be a discussion of the roles and responsibilities of the 'Information Commissioner's Office, often abbreviated to ICO. The ICO is the United Kingdom's independent body set up to uphold information rights and its mission is 'To promote public access to official information and to protect your personal information',[9] thus a discussion of this office is central to the theme of this thesis. The Netherlands' equivalent of the ICO is the Dutch Data Protection Authority or DPA, known as 'Autoriteit Persoonsgegevens' among Dutch speakers. Its mission, taken from the official Autoriteit Persoonsgegevens website, is to supervise "the processing of personal data in order to ensure compliance with the provisions of the law on personal data protection and advises on new regulations".[10] Taking the discussion of the ICO into consideration this section of the work will introduce the DPA and, following a discussion of its roles and responsibilities, will compare the ICO and Autoriteit Persoonsgegevens in terms of enforcement powers, responsibilities, and autonomy. Most importantly it will investigate how both Authorities are preparing for the changes in the incoming GDPR. The results of this comparison will then be applied to identify and suggest key areas of improvement that both authorities can adopt from one another, whilst arguing that the two roles are in fact very similar. The aim of this comparison is to better help us predict how the ICO may have to adapt in the future to better comply with European Data Protection Authority standards.

Considering the arguments and discussions set forth within this work the final aim of this thesis will be to conclude that the adoption of the GDPR in May 2018 by Member States of the European Union will have serious consequences upon the level of data flow and individual data protection within the United Kingdom due to 'Brexit', despite the United Kingdom's continuing attempts to maintain the same level of data flow between the UK and EU. This will lead eventually to a long-term weakening

[8] HM Government 2017, *The exchange and protection of personal data: a future partnership paper*, 2.
[9] Thomas 2008, 2.
[10] Autoriteit Persoonsgegevens 2018.

of digital business as it becomes a ‘third country’ and begins to lose its grip on its position as a world leader in digital data protection and digital economy. Using the comparison of the Dutch and British Data Protection Authorities it will aim to highlight the importance of these authorities and seek to argue that the best way for the United Kingdom to maintain some stake in EU data protection legislative decision-making is to utilise the knowledge and respect of the ICO as a bridge between UK and EU data protection legislation.

CHAPTER 1 – HISTORY OF EUROPEAN DATA PROTECTION LEGISLATION

i. Introduction

The right to privacy has always played a major role in European legislation and is one of the most important factors behind the constant re-development of legislation that responds and adapts to ever more complex personal data issues. This section thus aims to delve into the history of data protection laws and legislation within Europe, furthermore it will discuss comparable legislations from across the world that have influenced or been influenced by European legislations.

The first 'seeds' of data protection legislation within the EU were cast in 1950, when the 'European Convention for the Protection of Human Rights and Fundamental Freedoms' was drafted by the Council of Europe, entering into force in 1953.[11] Its Article 8 guaranteed the right of respect for privacy within family life, home, and correspondence for citizens of member states, and thus privacy protection entered official law. As the use of computers began to enter businesses and larger organisations following an increase in electronic data processing in the mid 1960's and 70's, the issue of maintaining the rights to privacy and protecting individual's data from manipulation began to be affected. Partly as a reaction to the growing demand for discussion of these issues, but also significantly as an attempt to reverse the United States' dominance within the field of the growing market of computers and processing within Europe, the European Parliament and European Commission decided to publish a Communication to the European Council in 1973, titled *Community policy on data processing*.[12] This Communication, which was primarily used to help the European industry become more globally competitive, put forward principles characteristics of data legislation that would be developed later on in the 1980's. It stressed harmonisation between national legislation of its member states and the need to adopt 'common measures for protection of the citizen'.[13] Furthermore, it understood the importance of finding a consensus among Member States early on to avoid being "obliged to harmonise conflicting national legislation later on".[14] This Communication would start the discussion of a single unified data protection and processing legislation within the EU which, by way of many unsuccessful attempts, would eventually lead to the GDPR, as will be discussed further below.

[11] Tikkinen-Piri *et al* 2017, 3.
[12] Fuster 2014, 112.
[13] Commission of the European Communities 1973, 13.
[14] Commission of the European Communities 1973, 13.

ii. 'Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing'

Upon completion of a report on 'the protection of the rights of individuals in the face of developing technical progress in the field of automatic data processing' in 1975 prepared by Lord Mansfield and linked to the Commission's 1973 Communication discussed above, the European Parliament adopted a resolution by the same name.[15] Within this resolution MEP's highlighted the necessity of a Directive on the matter so that a certain level of protection of member states' citizens would be ensured and normalised. Legislation such as this was at this point no longer a ground-breaking concept, as national and state data protection laws had already been established within the German state of Hesse in 1970 and on a national scale in Sweden in 1973, whilst national legislation in Germany and France would soon follow in 1976 and 1978 respectively.[16] In addition, the United States government had already passed their own personal data protection act through in 1974 titled the 'Privacy Act', which applied to federal agencies' record systems, and without a doubt influenced legislation both around the world and within the EU.[17] Due to this growing adoption of separate national legislation within EU countries the need for harmonisation within the EU became a pressing issue, and the European Parliament wished to get a harmonising legislation through as soon as possible. Following a second Resolution on the subject in April 1976 the 'Data Processing and Individual Rights Sub-committee' was set up and worked on the planning of European Council legislation in addition to a detailed investigation into the varied national data and privacy legislations found throughout Europe from June 1977 to March 1979, resulting in the 'Bayerl Report'.[18] Most notably the results of the Bayerl Report highlighted the strengths of the Austrian 'Federal Data Protection Law' of 1978 for its ability to grant Austrian citizens "a Constitutional right of personal data secrecy".[19]

iii. 1979 Resolution of the European Parliament

Taking into consideration the above-mentioned Bayerl Report and subsequent studies and investigations commissioned by the European Council the European Parliament, in 1979, chose to formally adopt the '*Resolution on the protection of the rights of the individual in the face of technical*

[15] Fuster 2014, 113.
[16] de Hert & Papakonstantinou 2017, 356.
[17] Privacy Act of 1974 [5 U.S.C § 552a].
[18] Fuster 2014, 117.
[19] Fuster 2014, 117.

developments in data processing'.[20] The key principles of the Resolution, which the European Parliament determined should be included in some form in any future EU legislation on data protection and processing, included a series of obligations imposed on data controllers, rights to be granted to all citizens of Members States to further protect their individual rights in the face of developing technical progress in the field of data processing, and perhaps most significantly the creation of a data control body of the European Community composed of 'a committee of representatives of the national bodies of the Member States responsible for the application of the legislation' and chaired by a European Parliament representative.[21]

iv. OECD Guidelines

Further attempts to creative effective harmony among the national data protection laws of EU member states came from the 'Organisation for Economic Co-operation and Development', abbreviated to OECD. The OECD issued guidelines in September 1980, setting out the following objectives:

- To achieve the acceptance of certain minimum standards of protection of personal data privacy;
- to reduce the differences between relevant domestic rules and practices in Member States;
- to avoid undue interference with flows of personal data between member countries;
- and to eliminate as much as possible reasons which might induce Member States to restrict trans-border data flows.[22]

As the guidelines were merely advisory and held no true legal substance their effectiveness was limited and reliance remained on individual countries' own particular national laws; a lesson that the EU would eventually learn from, as we will see from the GDPR.

v. Convention 108

One attempt, which would go on to play a large part later on in European data protection legislation was the enactment by the Council of Europe of the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', commonly referred to as Convention 108, in 1981.[23] As summarised by the Council of Europe itself, the Convention "is the first binding international instrument which protects the individual against abuses which may accompany the

[20] European Parliament 1979.
[21] European Parliament 1979, paragraph 13-14.
[22] Lynskey 2015, 47-48.
[23] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.

collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of data."[24] The legislation imposed responsibility to the processor and for the first time outlawed the processing of 'sensitive data' defined as race, health, sexuality, criminal record, and religion, in the absence of proper legal safeguards. The legislation also introduced restrictions on flow of personal data to countries with inadequate protection.

It is key to highlight the term 'binding' used in the Convention's summary as this legislation became the first of its kind to enforce its principles rather than using them solely in an advisory status. Unfortunately, the legislation was still not strong enough to be upheld as it required ratification from each member state before it could officially enter proper enforcement, this was its weakness. After a recommendation by the Council of Europe to ratify Convention 108 before the end of 1982, and with the added threat that the Council would propose its own legislation if member states failed to do so, only seven of its member states had done so by 1989, with divergence of the adoption of the legislation between these seven.[25] Interestingly, this recommendation for Convention 108 announced for the first time officially that data protection had the quality of a fundamental right, an announcement included in all but the English version of the text, which merely stated that; "Data protection is a necessary part of the protection of the individual. It is quite fundamental."[26] Though this may appear to be minor choice in wording, it is still a key reflection of the contrast in opinion that the UK Government had regarding data protection, a contrasting view with remnants that are still clearly visible today, as will be discussed within the third chapter of this work.

Convention 108 was a large step in the right direction for the European Union and its attempts at unified data protection legislation, but one not quite large enough. Lacking in the true fire power it needed to realise the EU's ambitions of harmonised data protection laws across the EU's Member States. Where Convention 108 succeeded however is in its role to further highlight the issues, which would further pressure the EU Parliament to take direct action and compose a new, more binding legislation.

vi. Schengen Information System

Demand for harmonisation was apparent not only among the European Parliament but also among Member States themselves, as several Member States took it upon themselves in intergovernmental co-operation agreements to tear down any 'borders' between them. The most significant result of

[24] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.
[25] Lynskey 2015, 48.
[26] European Commission, 1981.

this effort was the 'Schengen Agreement', a treaty aimed at the abolition of internal border checks, signed by Belgium, France, Germany, Luxembourg and the Netherlands in 1985.[27] This would later be amended in 1990 by the 'Convention on the Implementation of the Schengen Agreement', which detailed the introduction of a joint information system termed the 'Schengen Information System', or SIS. This system would connect national security departments, providing all agreeing member states with access to a large database on wanted and missing persons, preserving internal security between EU member states in the absence of physical border checks. Though it can argued that this was taking a step backwards in terms of freedom over personal data, the mere acceptance of Member States to openly share certain security information with each other demonstrates significant progress in terms of EU harmonisation. Furthermore, the Convention obliged users of the legislation to hold personal data entered for the purposes of tracing persons only for the time required to meet its original purpose or security requirements.[28] Since its official enforcement in 1995 it has grown from just the three Benelux countries, France, Germany, Portugal, and Spain, to its current form of 26 EU Member States and four associated countries participating in some form in the operation of the SIS, holding over 15 million reports on persons and objects.[29]

vii. Directive 95/46/EC

In the face of increasing pressure following particularly the failure of Convention 108, the European Commission felt they needed to introduce legislation that enforced data protection harmony among its Member States. Thus, as part of a package of legislation suggestions in 1990, the Commission put forward a proposal for the Directive that would go on to become Directive 95/46/EC[30] in addition to a proposal for a Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, and a request for a mandate to negotiate with the Council of Europe in order to adhere to Convention 108, which so far, as demonstrated above, had failed to have any degree of impact.[31]

As already discussed, in terms of working towards this goal, the Commission's Proposal took influences from Convention 108 after it had been working closely with the Convention during its implementation and drafting. However, major influences can also been considered from the German Federal Data Protection Act and to some extent from the French Data Protection Authority.[32] It covered four main issues; conditions under which the processing of personal data is lawful, the

[27] Fuster 2014, 122.
[28] Convention implementing the Schengen Agreement 1990, Article 112.
[29] Brouwer 2008, 1.
[30] Lynskey 2015, 49.
[31] Christou 2017, 182.
[32] Christou 2017, 182.

rights of data subjects, the requisite of data quality, and the establishment of a 'Working Party on the Protection of Personal Data' used to advise the Commission on data protection issues.[33]

Prior to its official adoption in 1995 the Directive within this Proposal would see further amendments and adjustments following criticism and feedback by Member States. In particular, October 1992 saw the submission of a fully revised Proposal which had adjusted its main objectives to be even more consistent with Convention 108 and the European Convention on Human Rights; ensuring that Member States guarantee "the rights and freedoms of natural persons with respect to the processing of personal data, and in particular their right of privacy".[34] Changes were also introduced to the suggestion of placing a distinction between public and private sector, an alteration which the French had requested; and the notion of processing was introduced to replace the notion of data file, as well as an increased emphasis on consent.[35] Many of these changes however appeared to be mostly focused on a different form of wording the same issues than any significant alterations. The 1992 Proposal was followed by further changes after the United Kingdom, Germany, Ireland, and Denmark showed their individual disapproval to certain factors in the 1992 Proposal.

1995 saw the adoption of the final agreed upon composition of the European Commission's Directive 95/46/EC, also known as DIR95. After years of investigations, studies and discussions between its Member States the EU succeeded in establishing this landmark legislation, which as we will discover, paved the way for the upcoming GDPR. The legislation was requested to be implemented by 24th October 1998, giving EU Member States three years to adopt and incorporate the legislation into their own national laws.[36] Once again, implementation took longer than expected, as only Sweden met the 24th October deadline.[37] The two primary objectives of the passed DIR95 were set out within its Article 1, stating as follows; "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" and "Member States shall neither restrict nor prohibit the free flow of data between Member States for reasons connected with the protection afforded".[38] These two objectives worked in partnership to ensure strong support economically –

[33] Fuster 2014, 126.
[34] Council of the European Communities 1992, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Article 1.
[35] Fuster 2014, 128.
[36] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Amendment 69.
[37] Carey *Data Protection: A Practical Guide to UK and EU Law* 2009, 6.
[38] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 1.

facilitating the establishment of the internal market through an uninterrupted data flow, and support for the rights of the EU's citizens – by establishing official lawful protection, in particular of the right to privacy, of fundamental human rights.[39] It was clear that "data protection had ceased to be merely a human rights issue; it was also intrinsically linked to the operation of international trade".[40]

DIR95 applied to personal data processed wholly or partly by automatic means, and to data held manually within produced filing systems structured by reference to individuals, it did not however apply to areas outside of the EU, a vital difference with the upcoming GDPR.[41] Further differences between DIR95 and GDPR in terms of scope includes areas of 'public safety', defence and State Security.[42]

The principles relating to the following areas of interest set out within the Directive are discussed in the following sub-chapters.

viii. Consent

Processing of data may only be permitted with the unambiguous consent of the data subject unless;

- it is 'necessary for the performance of a contract to which the data subject is party';
- it is 'necessary for compliance with a legal obligation to which the controller is subject';
- it is 'necessary to protect the vital interests of the data subject';
- it is 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority'; or
- it is 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject'.[43]

[39] Lynskey 2015, 46.
[40] Bennett & Raab 2006, 93.
[41] Carey 2009, 7.
[42] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 3.
[43] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 7.

Furthermore, the processing of personal data which would reveal such categories as ethnic origin, political opinion, religious belief, trade-union membership and health or sex life was to be prohibited unless certain factors discussed in Article 8[44] applied.

ix. Rights of the Data Subject

As well limitations to the data controller, DIR95 also granted many rights to the data subject, to demonstrate, the data controller must provide the data subject with at least these two key pieces of information; the identity of the controller, and the purposes of the processing of data. Additionally, any further information such as;

- 'the recipient or categories of recipients of the data'
- 'whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply'
- 'the existence of the right of access to and the right to rectify the data concerning him'.[45]

Furthermore, the Directive granted the data subject the right to object to the processing of data relating to him if compelling legitimate grounds are displayed, and to object 'on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed to a third party for the first time'.[46]

x. Data Protection Authorities

A key inclusion of DIR95 is the required creation of at least one or more supervisory public authorities per Member State tasked with the responsibility and main purpose of monitoring the application of the Directive within its territory. It is important to note that these authorities had to act with 'complete independence in exercising the functions entrusted to them'.[47] Evidence shows however that the freedom granted by the Directive created a wide scope in the interpretation of 'complete independence' in addition to the Data Protection Authority's powers between Member

[44] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 8.
[45] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 10.
[46] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 14.
[47] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 28.

States.[48] This was a direct result of the freedom afforded to Member States of being able to decide the final details of DIR95 under nationally implemented legislation, even though the goals set out in the Directive were supposedly binding.

xi. Article 29 Working Party

Accompanying the individual Data Protection Agencies was the creation of the 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data'. This would consist of a representative from each Member State's Agency and of the Commission and authorities established for the Community institutions. The board was to have advisory status and act independently.[49] The Working Party thus essentially acted as the hub for anything relating to the DIR95 legislation within the EU Community, making recommendations and providing feedback on aspects of the law that it felt needed addressing, due to the inclusion of representatives from each Member State these recommendations were taken seriously though technically the Working Party had no enforceable legal power.

xii. Sanctions

In terms of consequences from breaching these rules Article 24 of DIR95 states that 'Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive'.[50] Additionally, if a controller was found liable for damages suffered by a data subject as a result of unlawful processing, Member States were required to provide suitable compensation to the data subject in question.[51] Though these rules existed it is crucial to note the choice of wording; adopting 'sanctions' rather than explicitly mentioning fines allowed for a measure of discretion within the Member States to adopt their own form of fining system, which led to large discrepancies between each Data Protection Agency. The GDPR on the other hand is more forceful in its sanctions, with an ability for more severe fining powers, discussed further below.[52]

---

[48] Schutz 2012, 10.
[49] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 29.
[50] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 24.
[51] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 23.
[52] Grant & Crowther 2016, 288-289.

xiii. Data Protection Act 1998

DIR95 was implemented into UK law by the 'Data Protection Act 1998' which replaced the 1984 Act and provided until now the legal framework for data protection in the United Kingdom.[53] The Act received clearance on 16th July 1998 but did not come fully into force until 1st March 2000.[54] As already mentioned, the authority charged with enforcing this legislation within the UK was the ICO. The United Kingdom faced perhaps an easier transition into the DIR95 rules than most other European countries because it already been confronted with similar rules within its 1984 Data Protection Act. For example, any data processor within the United Kingdom would feel familiar already with the presence of the ICO as the 1984 Act had already introduced the requirement of registering with a Data Protection Authority titled the 'Data Protection Registrar'.[55] Similarly, a data subject already had the right since the 1984 Act to request access to any personal data that was held about him, with an obligation from the data user to supply this information within 40 days, though a small fee did apply for requests.[56] The Data Protection Act of 1998 set out eight principles relating to those in the DIR95 legislation, the importance of which were highlighted by the powers of the ICO. The principles were as follows;

- 'Personal data shall be processed fairly and lawfully'
- 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'
- 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.'
- 'Personal data shall be accurate and, where necessary, kept up to date.'
- 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'
- 'Personal data shall be processed in accordance with the rights of data subjects under this Act.'
- 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

[53] Woodhouse & Lang 2017, 3.
[54] Carey 2009, 9.
[55] Carey 2009, 4.
[56] Carey 2009, 4.

- ‘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.’[57]

xiv. Wet Bescherming Persoonsgegevens

In the Netherlands meanwhile, DIR95 was implemented through the ‘Wet bescherming persoonsgegevens’, known in English as the Dutch Personal Data Protection Act. The act was agreed upon in principle on 6 July 2000, but was not fully implemented until 1 September 2001, though it was revised considerably in January 2016.[58] The main alterations made during this revision were the introduction of an obligatory security breach notification to the data controllers and processors, and increased powers for the Data Protection Agency, further discussed below.[59] The authority charged with the enforcement of this legislation in the Netherlands was originally called ‘College Bescherming Persoonsgegevens’, though this was changed to ‘Autoriteit Persoonsgegevens’ in the 2016 revision. The authority is also known as the ‘Dutch Data Protection Authority’, to English speakers. The Dutch Data Protection Act chose to stay as close to the principles of DIR95 as possible and did not stray independently as much as the British Data Protection Act 1998. Its most important principles, translated into English, are as follows;

- ‘Personal data are processed in accordance with the law and in a proper and careful manner.’
- ‘Personal data are collected for specified, explicit and legitimate purposes.’
- ‘Personal data may not be further processed in a way incompatible with the purposes for which they were collected.’
- ‘Personal data may not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the data were collected or for which they are further processed.’
- ‘Personal data may be processed only in so far as they are adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed.’
- ‘Any person acting under the authority of the controller or of the processor, including the processor himself, in so far as they have access to personal data, only processes them on instructions from the controller, unless required to do so by the law.’[60]

[57] Data Protection Act 1998, chapters 29 & 48.
[58] Eskens 2016, 224.
[59] Eskens 2016, 224-225.
[60] Hendriks & James Legal Translations 2016, 9-11.

As demonstrated, the principles of both the Dutch and the British Acts are very similar in their aims, the direct result of the attempt by the EU to harmonise data protection laws throughout Member States through the DIR95. Further discussion of the ICO and Autoriteit Persoonsgegevens will continue in Chapter 4, paired with a direct comparison of the two authorities.

xv. Final Thoughts on Directive 95/46/EC

DIR95 was a well-planned and thought out piece of legislation, and for its time covered many of the issues present in the 1990's, when only 1% of the EU population was using the Internet.[61] It adopted successful characteristics of its predecessors without including too many of their weaknesses. It appeased the demand for fundamental rights enforcement from such legislation as Convention 108 whilst creating a focus on economic growth and harmonisation between Member States and businesses within the EU, combatting United States' business dominance present within the EU markets in the 1970's and 80's. However, like any legislation based around technology, it failed to maintain relevance whilst technology advanced, and due to this became in many ways outgrown and obsolete. Furthermore, the freedom it granted to Member States in their adoption of certain aspects of the legislation and its sanctions, which in many ways could be viewed as a strength, became its downfall, and a reason for its evolution into the GDPR. I say evolution, rather than replacement, as it truly is an evolution. The GDPR, as will be discussed, is rather an updated and improved version of the DIR95, as many of the DIR95's key principles are still to be maintained within the enforcement of the GDPR in May 2018.

[61] Craig & de Burca 2015, preface.

CHAPTER 2 – GENERAL DATA PROTECTION REGULATION

i. Introduction

The developments of data protection and privacy laws within the EU discussed in the previous chapters have led to the creation of the 'General Data Protection Regulation', or GDPR, to become fully enforced in May 2018. As will be discussed within this chapter, the GDPR shares many similarities with its predecessor the Directive 95/46/EC, referred to as DIR95 within this work, but is among other things far more detailed, with DIR95 being only a quarter of the length of GDPR.[62] This section of the thesis however, looks not at those similarities but rather at the changes being introduced by the new legislation, to discover how they are going to be received by Member States and businesses throughout the EU. The strategies that both the Dutch and the British Data Protection Authorities hope to adopt in order to receive the GDPR will be discussed in Chapter 4. Firstly however, it is vital to note that the new legislation is a Regulation, and not a Directive. It is important to mention this because of the significant difference in implementation this brings with it compared to DIR95; Regulations are immediately applicable in each and all Member States, requiring no legislation on a local scale, Directives, meanwhile, must be implemented in Member States individually.[63] This has two effects; one, a Regulation causes more harmony across Member States as there is less room for individual alterations, meaning European-based organisation no longer have to consider variety in the law when crossing borders, hopefully causing increased data flow and business within the EU. Two, control is taken away from the Member States and re-channelled towards the centre of EU administration so that individual Member States must adjust their own laws in order to make room for the GDPR. The European Parliament hereby hopes to improve upon the mistake of granting too much freedom to its Member States, which became one of DIR95's major downfalls.

The major changes to be introduced within the GDPR in May 2018 will be discussed in the following paragraphs. Finally, a minor section of this chapter will discuss the GDPR's effects on the archives sector.

ii. European Data Protection Board

The GDPR will establish the European Data Protection Board, or EDPB. The EDPB shall replace the A29WP, Working Party, but will essentially play a similar role, being composed once again of a

[62] Lloyd 2017, 183.
[63] Carey 2009, 10.

representative of each supervisory authority and the European Data Protection Supervisor.[64] The EDPB shall play a crucial role in enforcing consistency throughout the implementation of the GDPR. The EDPB's role as an independent supervisory authority will ensure correct application of the Regulation, advise the Commission, issue guidelines, recommendations and best practises, in addition to maintaining a publicly accessible electronic register of decisions taken by supervisory authorities and courts on relevant issues.[65] An important task of the EDPB will also be to determine the lead supervisory authority in cases where it has not been found possible to do so.[66]

iii. Data Protection Officer

The Regulation will enforce a mandatory designation of a data protection officer, referred to as DPO. This rule will apply in cases where processing of data is carried out by public authorities or bodies, or the core activities of the data controller or processor consists of regular and systematic monitoring of data subjects on a large scale.[67] A group of companies may designate a joint DPO, and the DPO may be employed by the controller or the processor, or perform the tasks based on a service contract.[68] The DPO must be granted access to all personal data and processing operations of the organisation employing him or her so that the tasks can be performed fully, reporting only to the controller or processor's highest management level. The processor or controller must publish the contact details of the DPO so that data subjects can approach the DPO for issues related to the processing of their personal data and to the exercise of their rights. The most important tasks and responsibilities of the DPO as outlined in the GDPR are as follows;

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Member State data protection provisions;
- to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority;

[64] EU Parliament, GDPR Regulation, article 68.
[65] EU Parliament, GDPR Regulation, article 70.
[66] Lynskey 2015, 68.
[67] EU Parliament, GDPR Regulation, article 37.
[68] EU Parliament, GDPR Regulation, article 39.

- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.[69]

The introduction of mandatory DPO's should have the effect of improving data protection awareness at company level, not only for the data controllers and processors, but indeed, and perhaps most importantly, for the employees and data subjects, who previously may not have had the opportunity to discuss their personal data rights previously. The need for improvement from DIR95 is displayed by statistics collected by the European Commission which show that only a third of employees in the EU feel well informed about their personal data protection rights, with only half of employees trusting their employers.[70] In addition, only 13% of 4800 data controllers interviewed in 27 EU Member States stated that they felt familiar with the national data protection law.[71] Clearly this introduction in the GDPR is a welcomed one, which will significantly improve legislation implementation within organisations and improve employer-employee relationships within business in regards to privacy rights. The DPO will only maintain this success however, if its role is respected and held with enough distance from the organisation itself so that it can maintain independence. The DPO position is already present in some EU Member States, thus the introduction is not ground-breaking, though the EU clearly feels the DPO has had success where it has been present to a degree where universal adoption is what they believe to be the answer. Germany, where the role is already mandatory, leads the EU with an impressive 700,000 registered privacy officers, in comparison the Netherlands, where the role prior to the GDPR is not yet mandatory, has 722 officers.[72] Furthermore, the new legislation will create a huge demand for individuals with a deep understanding of data processing operations and expertise in national and European data protection laws and practices. To keep up with this demand, and to avoid the potential of massive fines for non-compliance the national supervisory authorities must promote and ensure sufficient and regular training for DPO's. For the United Kingdom specifically it will be vital to maintain clear awareness of European data laws in addition to their own national laws. The GDPR however does not mention any specific qualifications that DPO's will need, leaving this decision to the individual hiring companies.

iv. Sanctions & fines

Arguably the most effectual and anticipated change will be the introduction of massive, and some fear, crippling, fines for infringement of the provisions stated within the Regulation. The newly

[69] EU Parliament, GDPR Regulation, article 39.
[70] Fritsch 2015, 149.
[71] Fritsch 2015, 149.
[72] Custers *et al* 2017, 7.

introduced fines, which businesses and institutions will be subject to from 25 May 2018, could amount to up to 20 million euros, or 4% of the offending organisation's total worldwide annual turnover, whichever is highest.[73] This brings the EU much closer to the fining powers of the U.S. Federal Trade Commission, which has previously imposed fines of up to $32.5 million.[74] The extent of the fine will depend on the severity, history of previous infringements by the offender, category of personal data affected, and any co-operation shown by the offender to mitigate the damage caused. This is a drastic change from DIR95, which did not impose specific fines itself but gave the data protection authorities of each Member State the freedom to impose fines as they saw fit within their own country. The British Information Commissioner's Office is perhaps the best example of an agency which has adopted measures to ensure its full authority and improve its public perception, and this will be discussed in depth further below. The freedom granted by the DIR95 within the enforcement of its sanction rules worked only for some Member States, as others remained very timid in their choice to fine, resulting in disparities between Member States' fines as large as 750,000 euros.[75] Overall, then, the sanctions imposed by DIR95 were not as effective as first hoped, leading to uncertainty within multi-national processor organisations, and a certain lack of respect of the laws imposed by the Directive through the Data Protection Authorities.

Whereas in DIR95 only data controllers were liable to any fines, data processors, in the GDPR, will now also face these same fines for infringement of the Regulation's laws. It is clear that the large increase in fining power is a message specifically aimed toward large-scale multinationals to take the new Regulation very seriously, due to the previous fine amounts being a mere dent in the company's total turnover. In addition to the economic disadvantage of being fined, businesses will also face receiving bad publicity, which could result in even further economic loss, and as demonstrated by British telecoms giant TalkTalk which in 2015 failed to protect customer data from a cyber-attack,[76] the dent to the customer relationship could take years to repair, if at all.

v. Increased territorial scope

Along with the increased fining powers of the GDPR the Regulation and its principles will now apply to a much wider territorial scope than previously. In addition to the Regulation applying to the processing of data and further activities by a controller established within an EU Member State, a rule already present in DIR95, the GDPR will now also apply its rules to the processing of data by

[73] EU Parliament, GDPR Regulation, article 83.
[74] Grant & Crowther 2016, 301.
[75] Grant & Crowther 2016, 301.
[76] Information Commissioner's Office 2016.

controllers or processors that are established outside of the EU, as long as they offer goods or services to EU data subjects or monitor the behaviour of data subjects within the EU.[77]

This is an important change, as not only will it affect Member States of the EU, but it will apply to organisations in almost every country in the world. Most importantly, it will increase the security of data subjects in the EU. The change will also end attempts by multinational organisations who previously were able to avoid DIR95 laws by placing their establishment outside of the previous scope of the DIR95. One downside of this increase in territorial scope may be that companies from outside of the EU will be less inclined to offer goods and services to citizens of EU Member States, for fear of failure to adhere to the GDPR's laws, especially with the increasing digital markets available elsewhere across the world. The majority of businesses, will not however be deterred by the GDPR, as the digital business opportunities available in the EU are so great in comparison to other less-developed parts of the world that the reward will be worth the added effort and risk.

vi. Increased rights of data subjects

One of the central aims within the Commission's proposal for the GDPR was to make "the exercise of data protection rights by individuals more effective".[78] The GDPR seeks to achieve this by adding new rules, in addition to specifying already present rights further and including further conditions, these include but are not limited to;

- New conditions for the data subject's right to obtain erasure or restriction of his or her personal data, providing the 'right to be forgotten' without the grounds previously required by DIR95.[79]
- The right to data portability, a new right that will greatly improve freedom for customers, but which may have a negative effect on smaller companies who rely on personalisation. It allows the data subject the right to receive the personal data concerning him or her from a controller, in a structured, commonly used and machine-readable format. Most importantly, this new right permits the data subject to transfer his or her personal data directly from one controller to another without hindrance from the original controller.[80] As already mentioned, this will allow customers more freedom when choosing service providers or any other business that requires personal data, allowing them to search for the best deals without being deterred by the hassle of inputting new data. It will however, reduce traffic to

[77] EU Parliament, GDPR Regulation, article 3.
[78] Lynskey 2015, 36.
[79] EU Parliament, GDPR Regulation, article 17 & 18.
[80] EU Parliament, GDPR Regulation, article 20.

smaller businesses which rely on personalisation but who may not be able to compete with the lower prices of larger competitors, businesses such as start-up fashion websites for example.

- The data subject will be more informed than ever about their personal data. Adding considerably to the provision of information already required by DIR95, the GDPR will require data controllers to also provide data subjects with the following additional information about the controller and data process: the contact details of the controller, its representative and DPO; the legal basis for the processing; the legitimate interests pursued by the controller or third party for data processing; source of the personal data, if not obtained from the data subject; the period for which the personal data will be stored, if possible; and whether the personal data will be disclosed to recipients in 'third countries'. Furthermore, the data controller must inform the data subject of their right to object to the processing, lodge a complaint with the supervisory authority, and withdraw consent to processing at any time.[81]
- Along with the increased transparency between data controller and subject, the data subject must be informed by the data controller with undue delay of a personal data breach in "clear and plain language" if the breach is likely to result in high risk to his or her rights and freedoms.[82]

As is demonstrated from the list above, the GDPR seeks to be much more explicit in its rights for data subjects compared to DIR95 as currently only 2 out of every 10 EU citizens claim to be informed about data collection and the way data are used.[83] There are however worries by some about the effects that the GDPR's 'right to be forgotten' will have on maintaining freedom of speech, claiming that freedom of speech has not been sufficiently considered in the principles of the new legislation. Jeffrey Rosen, a professor of Law at The George Washington University and one of the United States' leading voices in law, even goes as far as claiming that the GDPR "represents the biggest threat to free speech on the Internet in the coming decade".[84] He and former chief privacy counsel of Google, Peter Fleischer, argue that the strive for greater privacy is being used to justify ever greater censorship, highlighting scenarios in which the 'right to be forgotten' will cause threats to freedom of speech.[85] Even exemptions to this rule for artistic, journalistic or academic purposes may lack the strength to limit censorship across the Internet.

[81] EU Parliament, GDPR Regulation, article 13-15.
[82] EU Parliament, GDPR Regulation, article 34.
[83] European Union 2015, *Special Eurobarometer 'Data Protection*', 7.
[84] Rosen 2012.
[85] Fleischer 2011.

vii. Increased responsibilities of data controllers and processors

The GDPR places many more responsibilities onto the data controllers and processors than DIR95 did to increase cooperation with the supervisory authority. Before these responsibilities are discussed however it is important to mention the definitions of both the data controller and the data processor, as officially defined in Article 4 of the GDPR;

- Data Controller – "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".[86]
- Data Processor – "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".[87]

The newly introduced responsibilities for controller and processors include, among others, a new obligation to complete data protection impact assessments in instances when processing presents a high risk to the rights and freedoms of natural persons. This assessment, which will be completed with the assistance of the DPO, will essentially act as a risk assessment report that the national data protection authority can read in order to establish its allowance.[88] Previously, producing this document had been the responsibility of the national authority, as discussed in article 20 of DIR95.[89] This change may appear minor but could end up having a great impact on data protection overall as it will make data controllers and processors further aware of legislation and the risks apparent, whilst freeing up time and resources for the national data protection authority. Furthermore, controllers and processors will now be responsible for notifying the national authority of a personal data breach no later than 72 hours after becoming aware of it. This notification should contain at least the nature of the breach including the categories and approximate number of data subjects concerned, contact details of the controller or processor's DPO, the likely consequences of the breach, and any measures taken by the controller to address the breach.[90] As also mentioned under the increased rights of data subjects, if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject the controller must also notify the concerned data subjects without undue delay.[91] Again, I believe increasing the responsibilities of the controllers and

[86] EU Parliament, GDPR Regulation, article 4 (7).
[87] EU Parliament, GDPR Regulation, article 4 (8).
[88] EU Parliament, GDPR Regulation, article 35-36.
[89] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, article 20.
[90] EU Parliament, GDPR Regulation, article 33.
[91] EU Parliament, GDPR Regulation, article 34.

processors will prove advantageous for both parties, as not only will it reduce the workload of the national data protection authorities, it will most importantly result in increased cooperation and knowledge and awareness of GDPR principles within businesses and other organisations that handle data. The GDPR, in addition to the benefits that were just mentioned, also aims to improve the security of personal data through these measures by increasing the transparency between data controllers and data subjects.

viii. Summary of reforms

The above-mentioned introductions and reforms will go towards creating a system that in theory should harmonise and simplify the legal data environment across borders, evolving from 28 separate national laws to one single pan-European set of rules that must be adhered to, making it easier and less time-burdensome for both domestic and foreign companies to conduct their business within the EU. "Personal data is the currency of today's digital market"[92] is what former EU Commissioner for Justice Viviane Reding told delegates at a 2012 conference in Munich, and with its dual objectives the GDPR will aim to strengthen consumer trust in the digital economy and persuade more citizens to entrust online businesses with their personal data. In turn this will promote security and co-operation between Member States by giving individuals more control over their personal data.[93] The GDPR has the potential to become the leading data protection regulation in the world, one which may be replicated in countries across the globe if it can prove to provide a competitive advantage to businesses whose customers' confidence in their services has increased. We can already see a move towards this in regions outside the EU such as Asia, Latin America and Africa, where countries are updating existing data protection legislation as a response to a growing demand for stronger data security and privacy protection, harnessing the big opportunities apparent in a digital economy.[94] Not only will the GDPR's principles influence these regions, but most importantly its updated and improved framework for 'adequacy decisions' will allow EU businesses and data processors to be among the first to tap into to these newly developed digital markets, facilitating un-obstructed international data flow and trade.

[92] Rooney 2012.
[93] European Commission, *Communication from the Commission to the European Parliament and the Council – Exchanging and Protecting Personal Data in a Globalised World* 2017, 3.
[94] United Nations Conference on trade and development, *Data protection regulations and international data flows: Implications for trade and development*, 31-37.

ix. Effects on the Archives sector

Archival institutions, both private and public, will naturally also have to deal with the new rules introduced by the GDPR. Fortunately, however, archival lobbyists have been able to influence to a certain degree the drafting of the legislation throughout the creation of the GDPR, as such, the GDPR explicitly mentions archives and the exceptions to which they are part of. This is a welcome improvement from DIR95, which did not explicitly mention archives at all throughout the legislation, instead including it within the broad scope of "historical or scientific research" and its exceptions.[95]

The result of the efforts of archival lobbyists is demonstrated most visibly in Article 89 of the GDPR, titled 'Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'. As the name of the article suggests, Article 89 lists a number of safeguards which lay down a foundation for exceptions, making up the most explicit article within the legislation relating to archives. The articles to which Article 89 provides exceptions for are Articles 15 through to 21; the right of access by the data subject, right to rectification, right to restriction of processing, obligation of notification to the data subject regarding rectification or erasure of personal data or restriction of processing, right to data portability, and finally the right to object to processing.[96] Clearly then, the archival lobbyists were very successful in maintaining some freedom for archival processing during the age of the GDPR. This success however is tainted by the fact that these exemptions are invoked and implemented only by the choice of the Member State, thus the United Kingdom and the Netherlands could realistically choose not to implement archival exceptions, though with the strong voices of the national archives of both Member States this outcome would be very unlikely. Outside of the United Kingdom and Netherlands however, the flexibility granted by the GDPR, paired with the general vagueness and confusion surrounding archival terms within the legislation will most certainly lead to inconsistency between the rights of archives across the EU. It will be up to national archives of each Member State, and the European Archive Group established in 2006, to overcome these issues and create conformity so that cross-border research projects may do so without the added difficulty of complying with differing codes of conduct.

Article 40, though not explicitly mentioning archival practice, may provide the means for the development of such a shared set of codes of conduct for archival bodies across borders, which can be used to successfully implement the GDPR's new rules. This notion is supported by a Note from

[95] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 11.
[96] Taylor 2017, 187.

the European Presidency to the Council in December 2014, which says; "Codes of conduct may contribute to the proper application of this Regulation, including when personal data are processed for archiving purposes in the public interest… Such codes should be drafted by Member States' official archives or by the European Archives Group."[97] The United Kingdom could implement the GDPR's changes into their existing code of practice for archivists and records managers produced in 2007, similar to what the Netherlands has said it will do by continuing to follow a slightly altered 'Archiefwet' in conjunction with the 'Wet bescherming persoonsgegevens' and the 'Vrijstellingsbesluit Wbp'. It may make more sense however to completely overhaul the previous guidelines and work together with the European Archives Group and other Member States' archives to produce a new GDPR compliant guideline that can be followed across the EU. This would not only compliment the GDPR's aim to conform laws between Member States but would also create stronger opportunities for researchers and further transparency for individuals whose personal data is being archived.

Finally, some archives could also make use of the 'freedom of expression' exemptions granted in Article 85. Created to protect and support freedom of expression within journalism and artistic, academic or literary purposes the exceptions may also fall to include press and media libraries. This apparent 'loophole', which the Netherlands government intends to apply to the activities of many of its libraries and archives which hold materials relating to current affairs,[98] should also be adopted by other Member States such as the United Kingdom, to further relieve the constraints being introduced by the GDPR's other principles.

Though archives will survive the issues caused by the GDPR records managers and archivists will need to understand that personal data is being recognised more and more as personal property, with the GDPR seeking to embed this within the law archives must be prepared to alter the way they think about handling such data. In terms of archives the GDPR shows many improvements from its predecessor DIR95, most apparent being that archives are now given their own space within the legislation rather than being thrown in within the broad scope of historical and scientific research, yet archival associations still have a lot of lobbying to do to further cement recognition of the needs of archives in the face of ever-changing data protection laws. Most important among these is perhaps cementing a clear definition of 'archive' within the legislation, as currently the only definition that the EU has prepared is found within Recital 158 of the GDPR. The recital defines archives as: "Public authorities or public or private bodies that hold records of public interest should

[97] Taylor 2017, 187.
[98] White 2017.

be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest".[99] This definition, as Taylor argues, risks excluding archives, both private and public, that do not perform all of the activities mentioned from benefiting from the exceptions discussed in Article 89.[100] The urgency then, for the archival community to cement a clearer definition is significant if they wish to minimise the risk of smaller archives that fall outside of the current definition's scope to shut down due to confusion and the fears of facing the GDPR's significant fines.

In the opinion of Joris van Hoboken, professor of Law at the Vrije Universiteit Brussels, "The application of the GDPR to sectors such as the archiving sector illustrates the problems of having such a general law to solve such a wide variety of different issues related to personal data, in a wide variety of contexts."[101] Clearly the vagueness of how the GDPR has handled the archival sector within the legislation does highlight the weaknesses of an all-embracing legislation such as the GDPR, as noted by van Hoboken, yet the signs of improvement within the legislation from its predecessor prove that the understanding of the requirements of an archive in terms of data protection and processing is growing. Though it remains very vague, the exceptions that can be granted to archives prove that the voice of archives is being heard, and that the sector is still growing in recognition. Much like other businesses the incoming implementation of the GDPR demands a united archives sector that should be pro-actively formulating practises and codes of conduct to comply with the GDPR so that it can become stronger, rather than weaker, in the face of a new data protection environment. This will require cross-border cooperation and clear communication lines with individual Member States. On the individual archive level, archival institutions will need to be prepared to implement the requirements of the legislation such as employing a Data Protection Officer, and if not already the case, maintaining clear, verifiable written records of consent given by the individuals' whose data is being stored or processed.

[99] European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Recital 158.
[100] Taylor 2017, 185.
[101] Van Hoboken 2016.

CHAPTER 3 – HOW BREXIT WILL AFFECT GDPR ADTOPTION IN THE UNITED KINGDOM

i. Introduction

The GDPR's changes discussed in the previous chapter will have far-reaching effects throughout all EU Member States. This chapter aims to focus on the effects of the GDPR on the United Kingdom, highlighting aspects of the UK-EU data protection relationship. In particular it looks at what effects the decision to leave the European Union will have on British and EU data protection, privacy and co-operation following the UK's departure in 2019, and how the United Kingdom is going to implement the GDPR during this 'Brexit' transition period. It will also investigate whether the British government will choose a different data protection route entirely, discussing what the benefits and drawbacks of this would be. Regardless of what the UK government decides upon, many UK businesses may still be required to meet GDPR guidelines following the UK's withdrawal, coming as a result of the Regulation's increased territorial scope to include all organisations processing EU citizen personal data.[102]

Historically, the UK has been one of the most active EU Member States in co-shaping the EU data protection model, with the UK being among only the five other Member States that had ratified the EU Council's Convention 108 by 1990, and being represented in post-DIR95 legal work, Article 29 Working Group and even influencing key priorities within the new GDPR.[103] Furthermore, the UK's innovations in processing personal data for law enforcement purposes both prior to and following the terror attacks of 9/11 in the United States and July 2005 in London were instrumental in influencing and guiding contemporary EU law enforcement data protection guidelines.[104] However, though the UK has been such an key player in helping shape EU data protection signs that the UK does not fully support the ideals and notions behind the EU's visions of harmonisation appear to have been present far longer than since the 'Brexit' decision was made. Examples of British aversion to harmonisation are present most notably in the *Durant vs Financial Services Authority* case of 2003,[105] which resulted in a narrowing of the interpretation of 'personal data'; directly reducing the rights of individuals and creating uncertainty of the term's definition amongst other Member States. In fact, the UK's approach to EU data protection has always been to adopt EU directed legislation in their most minimalistic versions, criticising the overly complicated and bureaucratic nature of the EU's approach. Even the notion of treating data privacy as a human right, common in the EU,

[102] EU Parliament, GDPR Regulation, article 3.
[103] de Hert & Papakonstantinou 2017, 356.
[104] de Hert & Papakonstantinou 2017, 356.
[105] Durant v Financial Services Authority 2003.

conflicts with the more corporate British understanding of data privacy, where historically the general principle of 'invasion of privacy' has never truly been fairly recognised.[106] The UK's 'corporate' interpretation of a data privacy was further confirmed by research stating that "UK privacy leaders generally framed privacy protection as a form of risk management to avoid harm to consumer expectations" and "often define privacy protection in terms of fairness to customers and employees and managing risk."[107]

The terms of use and protection of data obtained or processed during this stage of 'limbo' before the UK's official withdrawal from the EU were published in the European Commission's position paper from September 2017,[108] stating that; "The United Kingdom or entities in the United Kingdom may keep and continue to use data or information received/processed in the United Kingdom before the withdrawal date and referred to below only if the conditions set out in this paper are fulfilled. Otherwise such data or information (including any copies thereof) should be erased or destroyed". Until the UK withdraws from the EU it will implement the Data Protection Bill 2017, which will align the UK's data protection laws with those laid out in the GDPR. The Data Protection Bill essentially duplicates the GDPR's principles but does include a few key derogations and exemptions which will be discussed in detail further below. The standards laid out in the 2017 Bill are also expected to remain fully aligned with the revised Convention 108.[109] The 2017 Data Protection Bill however has only been drawn up as legislation to carry the UK through this period of transition and will most likely be renewed after 2019, though a revised version of the Bill could be possible. Through this effort the UK government has declared its aims to remain in a good relationship with the EU in terms of data protection, whilst the temporary 2017 Bill will also buy more time for the UK government to construct a successful replacement come 2019.

Despite the apparent conflict in data protection ideology, and the decision to leave the EU in March 2019, the British government has stated that it wishes to build a "new, deep and special partnership"[110] with the EU and "retain its world-class regime protecting personal data".[111] So far however any extensive plans for what this will look like after the UK's full official split from the EU are unclear and hopeful at most, though the UK government has set out its priorities for the new EU partnership within its *Future Partnership Paper*, and has stated that it would like to agree early in the

[106] Lynskey 2017, 216.
[107] Bamberger & Mulligan 2015, 6-12.
[108] European Commission 2017, *Position paper transmitted to EU27 on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date*.
[109] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 5.
[110] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 6.
[111] House of Lords Hansard 2017, col 6.

process to mutually recognise each other's data protection frameworks,[112] believing this to be most beneficial for both sides to secure stability. The UK's priorities for the partnership are as follows;[113]

- Maintain the free flow of personal data between the UK and EU.
- Offer sufficient stability and confidence for businesses, public authorities and individuals.
- Provide for ongoing regulatory co-operation between the UK and EU on current and future data protection issues, building on the positive opportunity of a partnership between global leaders on data protection.
- Continued protection for the privacy of individuals.
- Respect of UK sovereignty, including the UK's ability to protect the security of its citizens and its ability to maintain and develop its position as a leader in data protection.
- No unnecessary additional costs to business.
- The model must be based on objective consideration of evidence.

ii. The Adequacy Model

The most prominent suggestion thus far that would adhere to this, at least from the UK side, has been a specially constructed form of the EU's adequacy model. The existing adequacy model was set out initially in DIR95 and was continued and expanded within Article 45 of the GDPR. The model allows for the transfer of personal data to and from a 'third country' or international organisation without the requirement of any specific authorisation per transfer. In addition to adequacy decisions covering all transfers of personal data to a third country, a partial adequacy decision can also be made, which would cover only the transfer of personal data from specific sectors of the third country's economy.[114] Again, this is an option that the UK could seek if the requirements for full adequacy could not be met, as it would, at the very least, protect the UK's critically important financial sector in principle. Adequacy decisions however, which follow the adequacy assessment, are time-consuming and very difficult, on certain occasions taking over a year to complete, and with the new expanded rules of the GDPR, the decision would have to be reviewed at least every four years to determine whether the third country is still suitably constructed to be considered adequate.[115] Furthermore, the UK would need to have another set of legislation prepared and in place when it leaves the EU as a request for adequacy cannot be made until the UK is officially enters

[112] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 8.
[113] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 6.
[114] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 9.
[115] EU Parliament, GDPR Regulation, article 45.

the status of a third country. Potentially, a solution to this issue could be to extend the 2017 Data Protection Bill until adequacy status has been granted, this approach would at least secure proper protection for individuals' data protection rights until adequacy was granted.

Aside from the adequacy decision, the UK may also be able to ensure data flow with the EU if the appropriate safeguards are adopted, these include;[116]

- Standard data protection clauses, available to view upon the EU Commission's website.
- Legally binding corporate rules approved by the appropriate data protection authority.
- An approved code of conduct.
- A set of approved certification mechanisms.

Failing these safeguards and a successful adequacy decision the UK could potentially be forced to commit to transfers of data based on 'derogations',[117] which allow transfers only in very specific cases. It is unlikely however that the UK or the EU would allow the relationship to dissolve to this point, as this limited form of data transfer would have extremely detrimental effects on both parties' digital economies.

iii. Privacy Shield Agreement

A final alternative to the adequacy model could be a model based closely upon the 'Privacy Shield' agreement that is currently in use between the EU and the United States.[118] This agreement replaced the 'Safe Harbor' agreement but took around two and a half years to be fully formulated, time that the United Kingdom, with Brexit looming in March 2019, simply does not have.

Though the UK has stated that its future data protection principles will remain aligned to the updated Convention 108 it has also stated multiple times that it will seek to exclude the Charter of Fundamental Rights from any EU retained law after Brexit.[119]

Like much of the Brexit negotiations, the UK's extremely egotistical and to a certain extent 'greedy' stance seems to have affected even the negotiations on data protection as the British government has stated within its *Future Partnership* paper that it aims to remain involved within future EU regulatory dialogue through its national data protection authority, the ICO, whilst also maintaining

[116] European Commission 2018, *Notice to Stakeholders: Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection*.
[117] European Commission 2018, *Notice to Stakeholders: Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection*.
[118] European Commission 2016, *European Commission launces EU-U.S. Privacy Shield*.
[119] Woodhouse & Lang 2017, 10.

complete responsibility over the content and direction of data protection policy and legislation within the United Kingdom's territories.[120] If the UK wishes to remain involved in some form within EU regulatory talks it needs to adopt a much more flexible stance on its own data protection legislation and be more open to the very likely possibilities that it may lose significant power in terms of influencing European data protection legislation.

iv. Consequences of failure to reach agreement

The potential consequences that will be met by both the UK and EU for failure to reach an agreement on data flow between the two parties could be severe. The UK, as the chart below displays, has the largest internet economy as a percentage of its GDP within the G20 countries, this huge reliance on its internet economy could result in huge losses in the UK's overall GDP if the internet economy was to be affected by the instability caused by both Brexit and the GDPR, and it most certainly will be affected. On the other hand, its large lead in internet economy compared to others may allow for some losses in the overall percentage without damaging overall British GDP too much, compared to the damage it would cause to other economies, though unfortunately the first possible outcome is far more likely due to the UK's reliance on this sector.

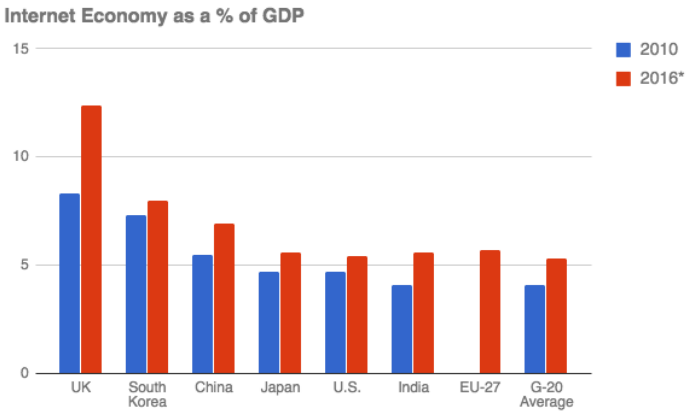

*Figure 1. BCG Internet Economy in the G-20 Report (2012), * 2016 are projected figures from when it was measured in 2012.*[121]

Further estimates predict that data economy will benefit the overall UK economy by up to £241 billion between 2015 and 2020,[122] with 75 percent of the UK's cross-border data flows currently

[120] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 7.
[121] HM Government Department for Digital, Culture, Media & Sport 2017, *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, 4.
[122] HM Government Department for Digital, Culture, Media & Sport 2017, *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, 5.

partnered with EU Member States it once again proves vital to maintain this unhindered flow of data if the UK wishes to avoid reductions in these numbers and its overall economic growth.[123]

It is not only the UK that would suffer from these losses. In losing the world leader in internet economy and data protection, the EU and companies within the EU that have been transferring their data with those in the UK will also be hard hit. The UK due to its advanced internet economy and expertise in data legislation is the top EU destination for tech company start-ups demonstrated by the fact that 17 out of the 40 European tech companies valued at $1 billion or more started in the UK. [124] If a suitable data transfer agreement is not concluded between the UK and the EU both parties will certainly suffer, the UK will lose its appeal as centre for tech start-ups whilst the EU will lose some of its largest tech companies. Aside from the economic factors the EU would also lose one of its key contributor's in data legislation debate and planning. Furthermore, free flow of data has been essential in fighting and preventing serious crime and terrorism over the last few years, if this were to be disrupted both the UK and the EU could miss opportunities to prevent deadly attacks and protect citizens. Between October 2014 and September 2015 alone the UK Financial Intelligence Unit received at least 800 requests from EU Member States,[125] if this partnership were to be lost, potential deadly consequences could follow.

Though there are many options that the UK could pursue, I believe the best option, if the UK wishes to maintain its position among data protection field leaders whilst maintaining its data market and businesses opportunities, halting the multinational company exodus from the UK to Europe and maintaining satisfactory data protection to its population, would be to align its domestic legislation as close as possible to the provisions laid down in the GDPR, possibly in a form similar to the UK's new 2017 Data Protection Bill. Though the EU may enforce certain sanctions on the UK, and the UK would most certainly be left with less decision-making power within the field of its data protection framework, it simply cannot afford to have its vital internet economy weakened by Brexit. Alignment with the GDPR would also persuade more large multinationals and tech start-ups to remain stationed within the UK. The UK understands that it is in a weak position, and the EU knows this too, it can therefore not afford to attempt to go it alone, like other Brexit decisions. The European Union would also be more welcome to the idea of maintaining a close relationship with the UK if it knew it had all the power. If the UK does not conform to the EU and GDPR principles it could find itself in a similar position as Jersey was in 2008, facing a lengthy battle to secure a much needed declaration of adequacy in order to maintain unhindered flow of data and protect a financial services sector that is

[123] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 3.
[124] House of Commons Business Innovation and Skills Committee 2016, *The Digital Economy*, 11.
[125] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 3.

of critical importance to the UK's national economy.[126] The drawbacks of this approach could very easily result in the United Kingdom having to continuously align its domestic data protection laws with EU laws every time the EU amends or updates them, and the UK, due to its new position as a third country, would no longer have any say or influence in these proposed amendments, resulting in the UK having to adopt laws that may not be in their best interest, unless of course a special relationship with exceptions is formulated.

v. British deviations from GDPR guidelines

Though the GDPR is more binding than previous EU data directive DIR95 it still gives Member States some opportunities to make provisions for how its principles are applied in their country. The GDPR can almost be viewed as a template which EU Member States must include within their own national regulations. The 2017 Data Protection Bill therefore acts as an all-encompassing data protection system which will, among its own laws, include those stated in the GDPR. The Bill and GDPR are designed to be read alongside each other, but the Bill is not limited to only including the GDPR provisions. The UK has taken full advantage of this limited freedom with an eye towards a United Kingdom outside of the EU, including several items not described in the GDPR, which will be discussed below. These modifications, which have been agreed upon by the EU, are designed to make the GDPR work for the benefit of the UK and its inhabitants, focusing specifically on areas such as academic research, financial services and child protection.[127] These deviations from the GDPR are also a sign of what future British data legislation could possibly look like, and must therefore be closely analysed.

vi. National Security

National security is outside the scope of the GDPR and is therefore one of the major areas where the 2017 Data Protection Bill deviates from the GDPR. The UK government includes within the new Bill both exemptions and modifications for the laws' application to UK national security and defence. The majority of these exemptions and changes are discussed in articles 26 and 110 of the Bill and grant the intelligence services of the UK large access to personal data in the name of 'national security'. The exemptions for national security will have a major part to play in the EU's decision to

[126] Lloyd 2017, 188.
[127] HM Government Department for Digital, Culture, Media & Sport 2018, *Data Protection Bill Factsheet Overview.*

grant the United Kingdom adequacy status post-Brexit as the EU appears to be wary about granting adequacy decisions to countries with over-reaching intelligence services with powers that grant them the ability to access personal data "beyond what was strictly necessary and proportionate to the protection of national security".[128] The EU's fear of the power of the UK intelligence agencies' ability to access citizens' data was further emphasised in a 2016 'tweet' by a major figure in the European Parliament and GDPR development, Jan Philipp Albrecht, who questioned the possibility of the UK's Data Protection Bill's rules on intelligence services being deemed adequate by the European Commission.[129] We have already seen a very similar issue occur between the EU and the US in 2015 as the European Union's Court of Justice dismissed the 'Safe Harbor' agreement, an agreement which had allowed for transfer of personal data between the EU and US, because of the US National Security Agency's particular ease of access to the personal data of thousands of EU inhabitants.[130] It is therefore a very real possibility that the EU would not agree to a UK-friendly adequacy decision unless they altered the exemptions present in the Data Protection Bill. Due to this concerning possibility, the ICO has stated that it will follow the debate on these exemptions to be reassured that the aim is not to grant a blanket exception for everything that the British intelligence and security services do,[131] though it is more likely that the ICO is merely saying this so that the UK has more chance to be granted adequacy by the EU. In any case, this could prove to be the largest hurdle for the British, in terms of data co-operation, to overcome.

vii. Additional offences

Two new offences which are not included in the GDPR are added into the Bill. The ICO has the ability to enforce sanctions for breaking these laws. They are:

- Article 171 – "It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data."[132]
- Article 173 – "It is an offence for a person listed in subsection (4) to alter, deface block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to

[128] Court of Justice, *Judgement of the Court: Maxamillian Schrems v Data Protection Commissioner*, 06 October 2015.
[129] Louis *et al* 2017, *Brexit and Data Protection: The UK government's new Data Protection Bill*.
[130] Court of Justice of the European Union 2015, *Press Release No 117/15, Case C-362/14: Maximillian Schrems v Data Protection Commissioner*.
[131] Louis *et al* 2017, *Brexit and Data Protection: The UK government's new Data Protection Bill*.
[132] Data Protection Bill, article 171.

receive".[133] In this case persons listed are the controller and a person who is employed by the controller.

viii. Child consent

Article 8 of the GDPR sets out the conditions applicable for a child's consent in relations to 'information society services'. The article sets the age at 16 but allows for some deviation as long as the age set is no lower than 13.[134] The UK government is not persuaded that setting the age at 16 would create any additional protections for children and thus has set its minimum age of consent at 13.[135] This is again a deviation from the EU principle which demonstrates the UK governments' more business-like approach to data protection by disregarding any data safety benefits for children which could occur if the age of consent was at 16, with an eye towards business and a larger consumer base instead.

ix. Processing of special categories of personal data

Article 9 of the GDPR sets out the specific circumstances under which 'special' categories, such as race, ethnicity, religion, trade union membership and even genetic and biometric data can be legally processed.[136] The Data Protection Bill will rely on these exemptions so that organisations particularly in the health and research sectors that have been processing sensitive personal data in compliance with the 1998 Data Protection Act can continue to do so under the new Bill and GDPR.[137] The new Bill will introduce a requirement that employers will need to have a 'policy document' in place during the period of processing, setting out their procedures for securing compliance with data protection principles and their retention and erasure policies.[138]

x. Processing of personal data relating to Criminal Convictions and Offences

Article 10 of the GDPR restricts the processing of personal data relating to criminal convictions and offences or related security measures to the control of an official authority "or when the processing

[133] Data Protection Bill, article 173.
[134] EU Parliament, GDPR Regulation, article 8.
[135] Data Protection Bill, article 9.
[136] EU Parliament, GDPR Regulation, article 9.
[137] HM Government Department for Digital, Culture, Media & Sport 2017, *Summary of GDPR derogations in the Data Protection Bill*, annex.
[138] Data Protection Bill, schedule 1 part 1.

is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects".[139] The UK aims to reflect the Data Protection Act 1998 as far as possible in this policy and the original Act classified criminal conviction data in the same definition as sensitive personal data. Therefore, the latest Bill intends to authorise the processing of this personal data in the same manner as the 'special' categories of personal data mentioned above, providing opportunity for processing otherwise than under the control of official authority, contrary to article 10 of the GDPR.[140]

xi. Automated individual decision-making

Article 22 of the GDPR states that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her".[141] The UK government feels that due to the fast moving pace of technology driving automated decision-making with algorithms and artificial intelligence it is essential to maintain some exemptions and safeguards to this rule. Therefore article 50 of the Data Protection Bill allows decisions to be made based solely on automated processing as long as they adhere to certain safeguards such as notification in writing to the data subject and allowing the right for this subject to request the data controller to reconsider its decision.[142] Again this is another example of how the EU intends to be much more individual-centric than the UK government.

xii. Processing and freedom of expression

Finally, article 85 of the GDPR allows for Member States to introduce their own exemptions and derogations to the GDPR's principles for the purposes of finding the right balance between protection of personal data and protecting the right to freedom of expression and information.[143] The 2017 Data Protection Bill therefore aims to reflect the Data Protection Act of 1998 as far as possible by presenting exemptions to processing specifically for journalistic, academic, artistic and literary purposes within Schedule 2 part 5 of the Bill.[144] Though as discussed in the previous chapter,

[139] EU Parliament, GDPR Regulation, article 10.
[140] HM Government Department for Digital, Culture, Media & Sport 2017, *Summary of GDPR derogations in the Data Protection Bill*, annex.
[141] EU Parliament, GDPR Regulation, article 22.
[142] Data Protection Bill, article 50-51.
[143] EU Parliament, GDPR Regulation, article 85.
[144] Data Protection Bill, Schedule 2, Part 5.

the introduction of the GDPR's 'right to be forgotten' will still present issues with freedom of speech even with the above-mentioned exemptions.

xiii. Why the ICO is the key to maintaining a close data relationship with the EU

The United Kingdom's best hope in maintaining a close and stable data relationship with the EU post-Brexit is by emphasising the importance of the Information Commissioner's Office, not only to other individual data protection authorities of EU Member States, but also to the EU as a whole. As discussed in detail within this thesis the ICO, and British governance in general, has played a huge and significant role in developing and fostering the concepts of data regulation both on a national scale and throughout the EU. The EU therefore needs the ICO, and the ICO, if it wishes to maintain relevance on an international scale, requires the EU as its platform. By reducing the United Kingdom to a third country the EU would be losing the important advice and guidance of the ICO, unless of course the EU accepts a relationship where the ICO still maintains some form of an advisory role within future data regulation and law discussions. The UK government has already stated that it wishes to adopt such a relationship with the EU following Brexit within its *Future Partnership* paper. Though, as was mentioned above, this may seem like an over-ambitious aim, a partnership such as this is indeed possible, and is unlikely to affect either the new 'independence' of the United Kingdom or the cohesion among remaining EU Member States, though compromise on both sides will be necessary for this to happen. Perhaps the largest challenge will be convincing the EU to agree to such a partnership, as granting such privileges to the UK may influence others to consider breaking away from the European Union. However, the EU Commission's call to develop international co-operation mechanisms to facilitate effective co-operation and enforcement of data laws by data protection authorities across the EU suggests that it would in fact be open to such a partnership in which the ICO could continue to share its expertise and relatively large resources with the network of EU data protection authorities. The UK government's *Future Partnership* paper suggests that within such a UK-EU model there should exist "an ongoing role for the UK's ICO in EU regulatory fora, preserving existing, valuable regulatory cooperation and building a productive partnership to tackle future challenges".[145] Importantly, the *Future Partnership* paper explicitly states that "The UK would be open to exploring a model which allows the ICO to be fully involved in future EU regulatory dialogue".[146] Essentially the ICO, within its nature as both an entity for and of the UK and the EU, could serve as a vital bridge between the UK and the EU. The ICO could even be considered as the

[145] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 7.
[146] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 7.

last EU outpost within the UK, helping influence UK data regulation with an eye toward the EU. On the other hand, the ICO could be considered, if the above-mentioned relationship is born, as the UK's last outpost of influence within the European Union, helping shape from a distance the future of data regulation within the EU into one that is UK-friendly. If the UK wishes to create this partnership successfully however it must move away from its current egotistical stance which has been so prevalent amid Brexit discussions thus far. Within the very same document that it stated its desire to remain among future EU regulatory dialogue the UK government also outlined its ambition to "continue to have responsibility for the content and direction of data protection policy and legislation within the United Kingdom". [147] Clearly it will have to compromise on one of these ambitions if it wishes to achieve the other. If it wishes to remain involved in some form within EU regulatory discussion it needs to adopt a more flexible stance on its own data protection legislation. Though the UK's role, if it achieves this, will be no more than advisory, it is certainly an improvement from being a mere onlooker.

[147] HM Government 2017, *Exchange and Protection of Personal Data: A Future Partnership Paper*, 7.

CHAPTER 4 – COMPARISON OF THE DUTCH & BRITISH DATA PROTECTION AUTHORITIES

i. Introduction

The following chapter will discuss and compare one of the most important aspects of data protection law in Europe; the data protection authorities. Specifically, this section of the work will aim to highlight and compare the functions, powers, and abilities of the British Information Commissioner's Office with those of the Dutch Autoriteit Persoonsgegevens. The final comparison drawn will consist of an investigation into how both authorities are preparing for the GDPR. The outcome of this comparison will be a summary of improvements that both data protection authorities could, and perhaps should, make to increase efficiency and be better suited to cope with the changes introduced by the GDPR. Most important to the outcome of this thesis' aims, the results will help us predict how the Information Commissioner's Office may have to adapt post-Brexit to further ensure full compliance with the European Data Protection Authority standards.

ii. British Information Commissioner's Office

This chapter will begin with a discussion of the British Information Commissioner's Office. The ICO has its roots in the in the Data Protection Act of 1984 which created the office of 'Data Protection Registrar', this was the UK's first independent body set up to supervise enforcement of the Data Protection Act. Following the arrival of the 1998 Data Protection Act this office evolved into what it is now known as today, with its powers have steadily increased since the body's conception. Its primarily role however, along with its mission to "promote public access to official information and to protect your personal information"[148] remains the same as it has always been. The strategic goals of the ICO, as laid out on its website are as follows;[149]

- "To increase the public's trust and confidence in how data is used and made available."
- "Improve standards of information rights practice through clear, inspiring and targeted engagement and influence."
- "Maintain and develop influence within the global information rights regulatory community."
- "Stay relevant, provide excellent public service and keep abreast of evolving technology."

[148] Thomas 2008, 2.
[149] https://ico.org.uk/about-the-ico/our-information/mission-and-vision/

- "Enforce the laws we help shape and oversee."

With offices in England, Wales, Scotland and Northern Ireland, the ICO processes more than 16,000 data protection complaints, 5,000 freedom of information complaints and over 200,000 calls to its helpline, in terms of data controllers it also administrates over 400,000 entries onto its register.[150] The body is currently led by the Information Commissioner Elizabeth Denham, appointed in July 2016 following the 7-year tenure of Christopher Graham. The terms of office for the Commissioner lasts a maximum of 7 years, re-appointment beyond this period is prohibited. The Commissioner and his or her office maintain the data rights of individuals by enforcing the laws set out in the Data Protection Act and any other relevant legislation. The ICO not only enforces the rules but also acts a source of information and advice, educating data controllers to improve overall data standards.[151] Importantly, the office is completely independent of the government, though it is sponsored by the UK Government's Department for Digital, Culture, Media & Sport. The ICO's autonomy ensures a fair policing of both the private and public sector, enforcing nation-wide adherence to the rules of the ICO. Its three core functions are to teach; providing policy advice to the British government, educating the general public, and promoting good practice by publishing Codes of Practice available to data controllers. It acts as judge, in a similar fashion to an Ombudsman, adjudicating on complaints and deciding the best course of action. Finally, it also acts as an enforcer; regulating, securing compliance, auditing, and prosecuting.[152]

iii. Autoriteit Persoonsgegevens

The Dutch data protection authority, which implemented the EU Directive 95/46/EC on 1 September 2001 through the Dutch Personal Data Protection Act known in the Netherlands as the 'Wet bescherming persoonsgegevens', was until 1 January 2016, when the Act was revised considerably, known as the '*College Bescherming Persoonsgegevens'* or CBP. Since the Act's revision it has been titled the '*Autoriteit Persoonsgegevens*'.[153] The official Dutch entity regarding personal data and its protection has its origins in an agency named 'de Registratiekamer', which was taken over by the CBP in 2001 and performed tasks similar to the Autoriteit Persoonsgegevens but with even less power. The most recent change in name, according to Chairman of the Authority from 1 August 2004 until 1 August 2016 Jabob Kohnstamm, better declared the new position of the body as a strict

[150] https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/
[151] HM Government Department for Digital, Culture, Media & Sport 2017, *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, 5.
[152] Thomas 2008, 2.
[153] Netherlands Government 2017, *Wet bescherming persoonsgegevens*, article 51 (4).

enforcer than the more general 'college', meaning 'board'.[154] This is a clear display of the evolution in Dutch data protection enforcement, and its enforcing authority, as along with the change of name the Autoriteit Persoonsgegevens gained a large increase in its firepower in terms of its ability to fine. Currently, the authority is led by Chairman Aleid Wolfsen, and Vice-Chairman Wilbert Tomesen who is charged with the supervision of the public and private sectors.[155]

The body's purpose is to supervise the processing of personal data in order to ensure compliance with personal data regulation laws. Amongst the laws being supervised are; the Dutch Data Protection Act, the Police Data Act, and the Basic Registration of Persons Act.[156] Its four core functions, as detailed on their website are as follows:

- Supervision; undertaking investigations assessing compliance with the law; acting as a mediator within disputes over the exercise of rights; maintaining a public register of notifications of processing operations; and assessing requests for granting exemptions.
- Providing advice; on legislative proposals and draft texts which significantly deal with the processing of personal data; and advising the Minister of Security and Justice on permits for personal data transfers to third countries which do not match the adequate level of protection.
- Providing information, education and accountability; information on how to interpret privacy legislation, publication of annual reports available to anybody, and to provide general information regarding the protection of personal data.
- International assignments; supervising the processing of personal data of Dutch citizens which takes place in another Member State, offering assistance to the DPA's of other Member States when requested to do so, active participation in Article 29 Working Party of data protection authorities and the joint supervisory bodies for Europol, Eurojust and European information systems.

Like the British ICO the Dutch Autoriteit Persoonsgegevens acts with complete independence, as required to do so by Article 28 of Directive 95/46/EC and continued into the GDPR.[157]

[154] Eskens 2016, 226.
[155] https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/de-leden-van-de-autoriteit-persoonsgegevens/mr-wbm-tomesen
[156] https://autoriteitpersoonsgegevens.nl/en/node/1930
[157]European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995, Article 28.

iv. Side-by-side comparison

In terms of operation size the UK ICO, if the individual state-level DPA's of Germany are not compiled, is by far the largest and most well-funded data protection authority in the EU, a result which matches the large economic interest of the UK in its internet data economy. With an estimated 26.5 million euros dedicated to it the ICO has a budget more than three times larger than that of the Dutch Autoriteit Persoonsgegevens, hiring 369 more employees than the Dutch figure of 73.[158] Furthermore the ICO is assisted in some of its duties by the 'Prudential Regulation Authority' and the 'Financial Conduct Authority', who act as regulators solely within the financial services sector. These statistics show that the ICO is capable of having a much wider-reaching effect within data enforcement. The ICO's much larger number of employees also remains so compared to the Netherlands even when the number of inhabitants of both countries are taken into account.[159] Though the Dutch Autoriteit Persoonsgegevens does gain a slight edge in budget when overall GDP of each country is taken into account the difference is almost negligible.[160] Analysis of these statistics would suggest that the ICO has a much larger presence within the knowledge of its country's inhabitants than the Dutch Autoriteit Persoonsgegevens has within its own, however research investigating the reputation of data protection authorities in the EU puts the Netherlands' Autoriteit Persoonsgegevens second only to Sweden's within the EU, concluding that 50% of Netherlands' inhabitants are aware of the entity, up from only 34% in 2010 and one of the largest increases in Europe. On the other end of the spectrum are the British; only 37% of UK inhabitants are aware of the presence and powers of the ICO, ranking the UK among the mid to lower half of the countries investigated, below many of the other larger EU economies such as Germany.[161] Though the majority of UK inhabitants may not be aware of the ICO, the 37% that are aware are highly active in voicing their data protection concerns, with the number of data protection concerns received by the ICO reaching just over 18,000 in 2016/17.[162] Furthermore, the fact that this number has been steadily rising since 2010/11 when it was just 13,000 is a sign that awareness of the authority and general personal data rights is growing. It is surprising however that the UK with its high number tech start-ups and considerable internet economy has such a low level of awareness. Of course, these statistics are not conclusive of which country has a more successful data protection authority, as many factors

[158] Custers *et al* 2017, 8.
[159] Custers *et al* 2017, fig. 3.
[160] Custers *et al* 2017, fig. 2.
[161] European Union 2015, *Special Eurobarometer 'Data Protection*', 52.
[162] *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, 5.

such as media attention, population density, and type of economy need to be taken into consideration, having said this, these figures should certainly not be ignored as they could lead to improvements for all involved.

v. Fining power

Perhaps the most important tool that data protection authorities can utilise is their ability to fine data controllers or processors that breach the data protection laws overseen by the authority. The EU clearly understands this as they have increased the maximum possible fine to up 20 million euros or 4% of the offending organisation's total worldwide annual turnover, whichever is highest.[163] However, until the new policies of the GDPR come into action in May 2018 the individual and varying fines of each Member State's authority still apply.

The Netherlands, and the Autoriteit Persoonsgegevens, had until revision of the Dutch Data Protection Act in January 2016 a relatively weak fining ability, able only to impose administrative fines of no more than 4,500 euros for a very limited set of violations including failure to notify the supervisory authority of processing operations and non-compliance with the full requirements of such a notification.[164] Fines of such insignificance were bound for failure as they lacked the firepower to grasp the attention of large multinational corporations or strike fear into repeat-offenders. The revised Dutch Personal Data Protection Act was in part created to resolve this issue, responding to a large number of incidents of personal data breaches in the Netherlands and providing the Autoriteit Persoonsgegevens with expanded powers. Since the reform, the Autoriteit Persoonsgegevens has been able to impose fines and penalties for non-compliance with the Data Protection Act of up to 810,000 euros or 10% of the offending company's annual turnover. Such a huge increase in its powers and authority elevates the Autoriteit Persoonsgegevens fining power from one of the EU's lowest to one of its highest, second only to the Spanish DPA's maximum fining power of 900,000 euros,[165] though depending on the offending company, the Autoriteit Persoonsgegevens 10% annual turnover rule may bring this to over 900,000 euros. Though this increase will garner increased respect for the Autoriteit Persoonsgegevens and its rules the Dutch authority is still limited to imposing such large penalties only in cases of intentional violation of the Personal Data Protection Act or, in cases of non-intentional violation, only after they have given the

[163] EU Parliament, GDPR Regulation, article 83.
[164] Eskens 2016, 225.
[165] Grant & Crowther 2016, 301.

data controller the instruction and opportunity to correct the violation.[166] This is a huge step for data protection in the Netherlands but will surely not be its last increase, with the new upper limits of fines being drastically increased in the GDPR we can expect not only the Netherlands but all other EU Member states that are serious about their data protection to increase their own fines.

Prominent examples of the fines and sanctions being issued by the Autoriteit Persoonsgegevens are as follows:[167]

- September 2014 – The DPA identified a company's violation of its terms as a result of providing tablets to elementary schools with a built-in app that monitored and processed study results of students, using the results for comparison purposes, in violation of the Personal Data Protection Act. Instead of fining the company the Autoriteit Persoonsgegevens chose to issue an official warning and continues to monitor the situation in case of further violations.
- January 2011 – The DPA concluded that the municipality of Charlois illegitimately processed data with regard to an individual's race for the purpose of maintaining a public order. The Autoriteit Persoonsgegevens ordered the municipality to cease processing of racial data within three days and delete this data from its database within three months, failure to adhere to this order resulted in an incremental penalty of 2000 euros per measure, and for each day that the order was not satisfied up to a maximum of 250,000 euros per measure.

These examples demonstrate that, although it now has serious powers of enforcement, the Autoriteit Persoonsgegevens prefers to limit fining, instead offering warnings and education as its key tools in combatting breaches in data protection.

In contrast, the British ICO has been one of the most active authorities among EU Member States in terms of imposing fines, even though its maximum penalty is significantly less than the Dutch. However, like the Autoriteit Persoonsgegevens the ICO's ability to impose any real sanctions or fines was relatively weak until an amendment in the UK Data Protection Act in April 2010 changed this. In fact, much like the Dutch system, the amendments made in 2010 were made solely to grant the ICO the power to issue fines.[168] Prior to the changes one of the only ways that the ICO could enforce the data protection laws was through measures aimed at remedying the practices of the data controller only after the breach had occurred.[169] In this scenario the ICO would serve an enforcement notice

[166] Baker & McKenzie 2016, 43.
[167] Baker & McKenzie 2016, 43-44.
[168] Grant & Crowther 2016, 288.
[169] Grant & Crowther 2016, 288.

requiring the data controller to rectify the mistake, failure to comply with these notices was, and still remains, a criminal offence and could be punished with fines up to £5,000. Since April 2010 the ICO has had the power to impose fines of up to £500,000 in cases where serious breaches of the Data Protection Act 1998 have occurred which could result or have resulted in substantial damage or distress and reasonable steps to prevent the breach have failed to be taken by the data controller.[170] From its introduction the ICO has not been afraid to impose its powers, which have grown every year since. Most recently the ICO gained further powers in the Digital Economy Act of 2017, which made it easier to enforce data laws against nuisance callers.[171] The ICO's firm approach was demonstrated in a 2010 speech by former Information Commissioner Christopher Graham, in which he stated "I will not hesitate to use these tough new sanctions for the most serious cases where organisations disregard the law."[172]

The high activity of the ICO in comparison with the Autoriteit Persoonsgegevens can be demonstrated by its most prominent issued penalties below:

- 30 September 2016 – British Telecoms company TalkTalk was fined £400,000 for security failings that allowed a cyber attacker to access customer data with ease, the largest ICO fine since its introduction.[173]
- 16 December 2013 – A loans company was fined £175,000 for sending millions of spam text messages.[174]
- 28 May 2012 – Brighton and Sussex University Hospitals NHS Trust was fined £325,000 after computer hard drives containing confidential personal data on thousands of patients were stolen.[175]

Though the above statistics are examples from the higher end of fines imposed by the ICO across a period of four years, the rate at which the authority imposes fines remains very high, and though the figures fluctuate year-by-year the total money raised from fines across 2011 to 2017 averages out at

[170] Baker & McKenzie 2016, 58.
[171] HM Government Department for Digital, Culture, Media & Sport (2017), *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, 6.
[172] Information Commissioner's Office, *Christopher Graham 2010 speech on new powers to issue monetary penalties*.
[173] Information Commissioner's Office (2016), *Data Protection Act 1998 Supervisory Powers of the Information Commissioner Monetary Penalty Notice to TalkTalk Telecom Group PLC*, paragraph 56.
[174] Baker & McKenzie 2016, 59.
[175] Grant & Crowther 2016, 289.

just under an impressive £2,000,000 per financial year.[176] This shows no slowing down either as the most recent statistics from 2016-2017 display the highest total yet, at just over £3,500,000.

The reasons behind the ICO's much higher rate of imposing penalties is unclear, but the fact that the ICO has a much larger number of dedicated staff may help explain how the ICO is able to handle and investigate more cases than the Autoriteit Persoonsgegevens. The UK's massive internet and data economy may also be a large influence on this, as a larger data economy means more data controllers to oversee. Lastly, I believe the fact that the ICO has only one chief Information Commissioner rather than the committee present in the Dutch system helps towards making decisions when it comes to imposing fines, providing the ICO with more opportunities to make its power felt.

vi. Leadership

In terms of leadership the two authorities are very different. As already mentioned earlier in this chapter the ICO is led by only one figure, appointed by the Crown. Currently it is Elizabeth Denham who holds the position of Information Commissioner, she is assisted in her statutory responsibilities by the Management Board, comprising of a General Counsel, two Deputy Commissioners and a Deputy Chief Executive, but ultimately has the final say in any important decision-making.[177] Autoriteit Persoongegevens on the other hand is led by a college of commissioners, consisting of a chairman and up to two other members. As already mentioned, these positions are currently held by chairman Aleid Wolfsen and vice-chairman and member Wilbert Tomesen, who were both appointed by Royal Decree upon nomination by the minister of Security and Justice.[178] The term of office for the chairman and other members is a period of 5 years, however this term is renewable by another 5 years upon re-appointment, 3 years longer than the maximum term of office for the British Information Commissioner.

The British ICO, in having a sole Commissioner in charge of everything data protection related, believes that combining the two responsibilities of promoting public access to official information and safeguarding personal information leads to a more efficient and balanced regime. As former Commissioner Richard Thomas noted in a speech at the Nationaal Archief from 2008 "it is best done

[176] HM Government Department for Digital, Culture, Media & Sport (2017), *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, 6.
[177] Information Commissioner's Office, https://ico.org.uk/about-the-ico/who-we-are/management-board/.
[178] Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/commissioners-dutch-dpa.

inside one office rather than having two Commissioners fighting over the boundaries".[179] The Dutch Autoriteit's leadership, in the form of a college of commissioners, appears to disagree with this British version. In its dual-shared leadership style it appears to favour a more democratic stance on policy enforcement, dividing the two responsibilities of promoting public access to official information and protecting personal information.

vii. Preparation for incoming GDPR

Both agencies have been hard at work in preparation for the upcoming GDPR, understanding the significance of a smooth transition both for the security of individuals' personal data and the maintenance of stability for businesses within the data economy.

The Information Commissioner's Office has been pro-active in its responsibility to prepare British inhabitants and companies for the changes coming in May 2018, specifically it feels it is important to maintain a calm and prepared persona, understanding the instability currently present in the UK due to Brexit. As part of this 'calm' persona Information Commissioner Elizabeth Dunham has made it clear that the ICO has no plans on making early examples of organisations by enforcing massive fines onto them for minor infringements, nor will maximum fines become the norm. She adds that the ICO will use its powers proportionately and judiciously and will use the other, less crippling, sanctions at its disposal such as warnings, where the ICO deems them to be more appropriate.[180] The tasks and responsibilities of the ICO will remain consistent throughout the introduction of the GDPR and new Data Protection Bill, while both the UK government and ICO's policy aim is to reflect the Data Protection Bill of 1998 as far as possible.[181]

Provided as a downloadable document from their website, the ICO has created the *Guide to the General Data Protection Regulation (GDPR)*, an extremely thorough 110-page guide produced by the ICO, specifically targeted at those who have a day-to-day responsibility for data protection, but open to anybody interested in the legislation. The main purpose of the guide is to cover and explain the provisions of the incoming GDPR in as simple a manner as possible so that organisations may understand and comply with the new requirements.[182] Discussed within the guide are the GDPR's principles, individual rights, accountability and governance, and exemptions, among many other

[179] Thomas 2008, 32.
[180] Denham 2017.
[181] HM Government Department for Digital, Culture, Media & Sport 2017, *Summary of GDPR derogations in the Data Protection Bill*.
[182] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

important topics.[183] It is a constantly evolving document which the ICO will be expanding and adding to until the official enforcement date of the GDPR. In addition to this guide the ICO provides many other tools that organisations can freely use to prepare for the GDPR, these include:

- A *12 steps to take now* checklist which advises data controller and processors on the 12 most important steps they should take in preparation.[184]
- Two separate self-assessment checklists which assess the high-level compliance of both data controllers, and data processors respectively.[185]
- A series of blogs posted by Information Commissioner Elizabeth Denham and others discussing some of the confusion and myths around the GDPR.[186]
- A podcast episode in which Information Commissioner Elizabeth Denham and Deputy Commissioner Steve Wood answer some of the questions raised by businesses worried about the GDPR.
- A dedicated advice-line offering small organisations preparing for the GDPR the opportunity to ring in for advice and answers regarding the GDPR and data protection laws in general.
- A number of sector specific FAQ documents answering questions that have been asked most often regarding the GDPR for small organisations, charities, educational institutions, small health organisations and local government.

If an organisation is still unsure about the effects and implementation of the GDPR the ICO also offers the opportunity to request advisory visits. These visits are available upon request for small to medium sized businesses, charities and not-for-profit organisations and involve a one day visit from an ICO representative who investigates the policies and procedures present to find areas for improvement. These visits also allow members of staff to ask questions regarding data protection and the GDPR.

In addition to the movement towards the GDPR following increased fines in the revision of the Dutch Data Protection Act in January 2016 the Dutch Autoriteit Persoonsgegevens has, like the British ICO, dedicated an entire section of its website to GDPR preparation and information. Unlike the ICO however, the Autoriteit Persoonsgegevens has not produced its own published and downloadable general guide to the GDPR which goes into such great depth as the British. Instead, it offers the

[183] Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
[184] Information Commissioner's Office, https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
[185] Information Commissioner's Office, https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/
[186] Information Commissioner's Office blog.

chance to download a 98-page in-depth GDPR guide produced by the Ministry of Justice and Safety. Perhaps the Netherlands, within its stable position within the EU as one of its long-time Member States does not quite feel the same sense of urgency and significance in providing Dutch companies with a sense of stability, as Dutch inhabitants and companies are not facing the same understandable confusion as that caused by Brexit. Furthermore, the relatively recent changes to the Dutch Personal Data Protection laws in January 2016 means that most companies will have already aligned themselves comfortably with the laws and principles being introduced in May 2018. We know that the recent changes in the Dutch Data Protection Act were brought in with an eye towards the GDPR at least, demonstrated by the sharp increase in the Autoriteit Persoonsgegevens' fining powers. Nevertheless, its GDPR dedicated section proves that the Autoriteit Persoonsgegevens are not taking the introduction of the GDPR lightly. The authority is providing advice, and the Dutch inhabitants and companies concerned are taking that advice. The two most downloaded documents currently on its website are both GDPR related. The first document is a *Prepare for the GDPR in 10 steps*[187] preparation checklist similar to the 12-step guide provided by the ICO, which provides the 10 most important steps a data controller or processor should be taking to prepare for the GDPR as a downloadable PDF document. The second most downloaded document on the Autoriteit Persoonsgegevens website is *The GDPR in a nutshell*, a very brief summary and overview of the changes being introduced within the GDPR.[188] These two documents, act together to provide the main bulk of authority produced introductory information to the GDPR. In addition to these two sources and the large in-depth guide by the Ministry of Justice and Safety there are more topic-specific guidelines available, produced by the Authoriteit Persoonsgegevens in conjunction with other EU data protection authorities. They are as follows;[189]

- Guidelines on the Data Protection Impact Assessment, includes a Dutch translation.
- Guidelines on the application and setting of administrative fines.
- Guidelines on the Data Protection Officers, includes a Dutch translation.
- Guidelines on how to identify a controller or processor's lead supervisory authority, includes a Dutch translation.
- Guidelines on the right to data portability, includes a Dutch translation.

[187] Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf
[188] Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_in_een_notendop.pdf
[189] Autoriteit Persoonsgegevens, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg#over-welke-onderwerpen-geven-de-europese-privacytoezichthouders-uitleg-in-guidelines-6189

- Guidelines on certification, expected to be published early 2018.

Furthermore, the Autoriteit Persoonsgegevens provides more information regarding the majority of the above-mentioned topics as webpages on its official website, included within this additional information are topic specific FAQ sections. A telephone number for the Autoriteit Persoonsgegevens is also provided, but it is not GDPR specific like that of the ICO, which offers its GDPR help-line for small business and organisations. Though it may not seem as approachable as the ICO, the Dutch authority is successful in not excluding anyone from accessing information, even providing a lesson-plan which provides the tools and information necessary to educate schoolchildren about their own personal data and privacy rights. Taught within three 45-minute lessons the plan offers a basic introduction to privacy and personal data, teaches children why organisations may be interested in their personal data, and informs them of their rights concerning their data, all available as a free download for interested teachers.

viii. Results of comparison

By comparing the approaches of both the ICO and Autoriteit Persoonsgegevens the latter appears to take into account the worries and changes applicable to the individual much better than the other. Through dedicating specific sections of its GDPR preparation to topics such as control over your own personal data and the GDPR in school, offering education over rights to children specifically, the Autoriteit Persoonsgegevens offers a more individualised approach to its preparation than the ICO. Overall however, I believe that the evidence as shown above, displays a much wider-reaching and more in-depth approach by the ICO in preparing its inhabitants and businesses for the changes coming in May 2018. The Autoriteit Persoonsgegevens fails to diversify its resources and learning tools as efficiently as the ICO has done but provides far more FAQ's on a wider range of GDPR topics than the ICO. The ICO fails to provide easy-to-understand information regarding the GDPR specifically for individuals apart from a summary of changes to child rights but excels in providing learning and advisory opportunities for businesses and organisation through its helpline and advisory visits. The ICO's focus on businesses rather than individuals could be due to the UK's current focus on keeping the organisations currently operating within its powerful internet data economy happy enough to be convinced against relocating to another Member State of the EU with Brexit fast-approaching.

FINAL CONCLUSION

The question of whether the GDPR is a suitably strong enough replacement to the European Union's previous data protection legislation Data Protection Directive 95/46/EC will not be answered until it has had a chance to officially work within the Union upon its enforcement in May 2018. However, the arguments set forth in Chapter 2 of this work do already demonstrate that it's by no means perfect, and that there are and will be flaws in parts of its principles. It's most worrisome flaw will likely be the new principle of the 'right to be forgotten' which, though it has many positive effects for those with information on the internet that they wish to be confidential, could on the other hand be viewed as a powerful tool for censorship which will have a much larger damaging effect on maintaining freedom of speech on the internet. It is clear then that the balance between maintaining privacy whilst promoting freedom of speech has yet to be struck even in the GDPR. It is up to the Member States of the EU to strive further towards finding this balance, especially as digital economies and leaders continue to grow, collecting more and more personal data, whilst individuals are creating more data per hour than ever before. Compared to its predecessor however it is a vast and necessary improvement which will, despite some of its flaws, succeed in promoting data business and digital economy both between EU Member States and with 'third countries' dealing with EU data. Most importantly it will also successfully bring individuals' data rights and protection within the European Union into the 21st century by giving individuals more knowledge and control over their own personal data and how it is processed. The GDPR has the potential to become the world's leading legislation in data protection and international governments both present and future may look toward the European Union to influence their own similar legislations. It is vital for the United Kingdom to not miss out on the power and influence that will be gained by Member States of the European Union during their adoption of the GDPR if they wish to maintain a strong influence within the data sector, as concluded in the discussions of Chapter 3.

This work's primary investigation was a look into how the effects of Brexit would affect not only the UK-EU relationship in terms of data transfer and protection but what the United Kingdom's plans are for implementing the GDPR until March 2019 and any other data protection legislation thereafter. The investigation in Chapter 3 found that during the stage of 'limbo' in between the GDPR's May 2018 full enforcement and the United Kingdom's continuing preparations towards officially leaving the European Union in March 2019 the UK government had prepared its own updated Data Protection Bill which would essentially align the UK's data protection laws with those proposed in the GDPR. Aside from the UK's priorities for a future partnership with the EU however, any truly concrete plans beyond March 2019 were found to be lacking. After an analysis and discussion into the benefits and drawbacks of the options available to the UK government the chapter concluded

that, in order to halt a mass exodus of tech companies leaving the UK to go to Europe whilst maintaining satisfactory data protection principles to its citizens it should align its domestic legislation as close as possible to the GDPR, possibly in a form similar to its current Data Protection Bill. This way it has the best chance to be granted adequacy status as a 'third country' by the EU, which in turn would allow data transfers between United Kingdom and the EU. A discussion of the Data Protection Bill's deviations however found that in order to reach such an agreement with the EU the UK must sacrifice a number of changes that it wishes to introduce into the GDPR's principles. In particular it was found that the UK must be willing to adjust its principles on national security, and the exemptions that it grants to the intelligence services of the UK to ensure that they cannot access personal data beyond what is strictly necessary. Finally, the chapter found that utilising its data protection authority, the Information Commissioner's Office, would be the UK's best chance to secure any kind of input in future data legislation discussions by highlighting the beneficial role that the office has held in European data legislation planning both in the past and in the present.

Finally, the fourth chapter continued upon the discussion of the Information Commissioner's Office and expanded upon it by investigating its role in comparison with that of the Dutch Autoriteit Persoonsgegevens. An analysis of the similarities and differences was drawn from this investigation to conclude how the British data authority system is different in both powers and the way it operates in comparison to a typical European data protection authority. The comparison would help us predict how the British data protection authority may have to adapt after Brexit to further comply with European data protection authority standards. The comparisons were also drawn to investigate whether either of the two authorities should adopt the other's principles in order to function more effectively during the GDPR's introduction and enforcement. The chapter continued the theme of highlighting the importance of utilising the Information Commissioner's Office as the key to an advantageous British relationship with the EU after Brexit. The comparison, which focused on fining powers, leadership, and preparation for the GDPR, concluded that with a much larger workforce and higher budget, combined with a management system led by only one leader, the Information Commissioner's Office was more able, and perhaps more inclined to issue very large fines to those that breached rules whereas the Autoriteit Persoonsgegevens appears to take a more 'warn first, issue a fine as last resort' type of approach, as demonstrated by both authorities' most prominent issued penalties from the last few years. The Autoriteit Persoonsgegevens should therefore seek to emulate the British one-leader style management system if it wishes to fully utilise the large fining powers that the GDPR will grant it. Aside from these differences, the chapter concluded that the two authorities do in fact share many similarities, a benefit then, for the UK if it wishes to maintain the ICO's connection to the EU as its bridge to EU legislation discussions. The final comparison, which

looked at preparations for the GDPR, found that both authorities had strengths and weaknesses in their approach to the GDPR. It showed a correlation between the UK's understanding of data protection as a business decision and the way that it is preparing its citizens and organisations for the changes of the GDPR. It concluded that the ICO's approach was more wide-reaching and in-depth, likely again due to the ICO much larger workforce and budget. An area of improvement for the ICO, and one which they should attempt to emulate the Autoriteit Persoongevens in, was a more individualised approach towards preparation, which the Dutch system succeeded in by producing GDPR teaching tools for children.

Careful consideration of the facts and discussions put forward within the arguments of this work concludes that the United Kingdom will indeed suffer significantly from the introduction of the General Data Protection's principles whilst it undergoes the process of Brexit. The particular areas that will feel the damaging effects of the UK's split from the EU's data protection legislation most will be the large internet economy of the UK, which will see drastic reductions in the rate of tech companies choosing to start up there, and the security and safety of individuals' personal data as Brexit will reduce cooperation between data security companies in the UK and EU. The United Kingdom has few options to halt these outcomes and prepare a stable plan for life post-Brexit, its best option, as concluded by the discussions of this thesis, is to focus on keeping the EU happy. It should seek to do this by aligning its data protection principles as closely to those laid out in the GDPR and, more importantly through promoting the beneficial importance of the Information Commissioner's Office's knowledge and expertise in data legislation planning to any future EU data plans. If the UK succeeds in maintaining the Information Commissioner's Office as some sort of last British bastion in the EU it will be able to make its voice heard and potentially have some say in any future EU data protection legislation discussions, allowing the UK to follow the GDPR's principles from the side-lines, knowing that any future changes will not be of detriment to the aims of the United Kingdom. To further increase the chances of maintaining this connection the ICO should adopt some of the characteristics of the Dutch Autoriteit Persoonsgegevens, so that it remains aligned with European data protection authority standards.

BIBLIOGRAPHY

Monographs

Bamberger, K. & Mulligan, D. (2015) *Privacy on the Ground, Driving Corporate Behavior in the United States and Europe*, London & Cambridge MA.

Bennett, C. & Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge MA.

Brouwer, E. (2008) *Digital Borders and Real Rights: Effective Remedies for Third-country Nationals in the Schengen Information System*, Leiden & Boston.

Carey, P. (2009) *Data Protection: A Practical Guide to UK and EU Law* (Third Edition), Oxford & New York.

Christou, G. (2017), 'European Privacy and Data Protection Policy', in Zahariadis, N. & Buonanno, L. (eds.), *The Routledge Handbook of European Public Policy*, Abingdon.

Craig, P. & de Burca, G (2015), 'Preface', in Lynskey, O., *The Foundations of EU Data Protection Law*, Oxford.

Fuster, G.G. (2014) *Emergence of Data Protection as a Fundamental Right of the EU*, New York & London.

Grant, H. & Crowther, H. (2016) 'How Effective Are Fines in Enforcing Privacy?' in Wright, D. & De Hert, P. (eds.) *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Switzerland.

Thomas, R. (2008) *Freedom of Information: The UK Experience*, Nationaal Archief, the Hague.

Lynskey, O. (2015) *The Foundations of EU Data Protection Law*, Oxford.

Lynskey, O (2017) 'Courts, privacy and data protection in the UK: Why two wrongs don't make a right' in Brkan, M. & Psychogiopoulou, E. (eds.) *Courts, Privacy and Data Protection in the Digital Environment*, Cheltenham UK & Northampton MA USA.

Schutz, P. (2012), *Comparing formal independence of data protection authorities in selected EU Member States*, Conference paper for the 4th Biennial ECPR Standing Group for Regulatory Governance Conference, Exeter.

Oral evidence

Hancock, M. (2017), 'Select Committee on the European Union EU Home Affairs Sub-Committee – Corrected oral evidence: The EU Data Protection Package', oral evidence by Matt Hancock MP Minister of State for Digital and Culture, Department for Culture, Media & Sport, House of Lords United Kingdom, 1 February 2017.

Hoboken van, J. (2016), 'The Right to be Forgotten seen from the perspective of the Right to Remember', presentation given at conference on the 'Right to be forgotten versus right to remember, Brussels, Belgium, 10 October 2016, accessed 24/04/2018, http://www.arch.be/index.php?l=en&m=news&r=confe%20rences&e=international-congress-right-to-be-forgotten-versus-right-to-rem%20ember&p=international-congress-10-october-brussels-right-to-be-forgotten-%20versus-%20right-to-remember.

House of Lords Hansard (2017), 'Queen's Speech 21 June 2017', col 6, vol 783.

Information Commissioner's Office (2010), *Christopher Graham 2010 speech on new powers to issue monetary penalties*.

Journals

Custers, B; Dechesne, F; Sears, A; Tani, T; van der Hof, S. (2017), 'A comparison of data protection legislation and policies across the EU', *Computer Law & Security Review* 33.

de Hert, P. & Papakonstantinou, V. (2017), 'The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit', *Computer Law & Security Review* 33.

Denham, E (2017), 'GDPR – sorting the fact from the fiction', *Information Commissioner's Office blog*, accessed 25/03/2018, https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/.

Eskens, S.J. (2016), 'New Notification Obligations and Fines under the Dutch Data Protection Act', *European Data Protection Law Review*, vol 2.

Fleischer P. (2011), 'Foggy thinking about the Right to Oblivion', *Privacy…?*, accessed 23/03/2018, http://peterfleischer.blogspot.nl/2011/03/foggy-thinking-about-right-to-oblivion.html.

Lloyd, I. (2017), 'IT Law in the United Kingdom after Brexit', *Computer Law & Security Review* 33.

Louis, F.; Braun, M.; Ratliff, J.; Benizri, I. (2017) 'Brexit and Data Protection: The UK government's new Data Protection Bill', *Wilmerhale Privacy and Cybersecurity Law Blog*, accessed 09/03/2018,

https://www.wilmerhale.com/blog/privacy-and-cybersecurity/post/?id=17179885471&utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

Rooney, B. (2012), 'Reding Details Sweeping Changes to EU Data Laws', in *The Wall Street Journal Online*, accessed 23/03/2018 https://blogs.wsj.com/tech-europe/2012/01/23/reding-details-sweeping-changes-to-e-u-data-laws/

Rosen, J. (2012), 'Response: The Right to be Forgotten', *Stanford Law Review Online*, 88, accessed 23/03/2018, https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/

Taylor, I. (2017), 'The General Data Protection Regulation ([EU] 2016/679): White Paper', *Archivar*, vol 72.

Tikkinen-Piri, C; Rohunen, A; Markkula, J. (2017), 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies', *Computer Law & Security Review: The International Journal of Technology Law and Practice*.

Zerlang, J. (2017), 'GDPR: a milestone in convergence for cyber-security and compliance', *Network Security*, vol. 6.

Legislation

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, ETS No 108, 28 January 1981.

Council of the European Communities, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, (92/C 311/04), COM (92) 422 final – SYN 287, 27 November 1992.

Court of Justice, *Judgement of the Court: Maxamillian Schrems v Data Protection Commissioner*, 06 October 2015.

Data Protection Act 1998, HM Government.

Data Protection Bill (2017), Bill 153, House of Lords and House of Commons.

Durant v Financial Services Authority 2003, [2003] EWCA Civ 1746.

European Parliament and Council Directive 95/46/EC of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* OJ L281/23 1995.

European Union (1990), *Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders*, Official Journal L239, 19 June 1990.

European Union (2016), *On the protection of natural persons with regard to the processing a of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Council of the European Union, Brussels, Belgium.

Hendriks & James Legal Translations (2016), *The Personal Data Protection Act*, Amsterdam.

Netherlands Government (2017), *Wet bescherming persoonsgegevens*, July 2017.

Privacy Act of 1974 [5 U.S.C § 552a], United States.

Government papers

Commission of the European Communities (1973), *Community policy on data processing (Communication of the Commission to the Council)*, SEC(73) 4300 final, Brussels.

Court of Justice of the European Union (2015), *Press Release No 117/15, Case C-362/14: Maximillian Schrems v Data Protection Commissioner*, Luxembourg.

European Commission (1981), *Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*, L246/31.

European Commission (2016), *European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows*, 12 July 2016, Brussels.

European Commission (2017), *Communication from the Commission to the European Parliament and the Council – Exchanging and Protecting Personal Data in a Globalised World*, 10 January 2017, Brussels.

European Commission (2017), *Position paper transmitted to EU27 on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date*, TF50, 14 Commission to EU 27, 6 September 2017.

European Commission (2018), *Notice to Stakeholders: Withdrawal of the United Kingdom from the Union and EU rules in the field of data protection*, 09 January 2018, Brussels.

European Parliament (1979), *Resolution on the protection of the rights of the individual in the face of technical developments in data processing*, OJ C140/34.

European Union (2015), *Special Eurobarometer 'Data Protection'*.

HM Government (2017), *The exchange and protection of personal data: a future partnership paper*, August 2017.

HM government Department for Digital, Culture, Media, & Sport (2017), *A New Data Protection Bill – Our Planned Reforms: Statement of Intent*, August 2017.

HM government Department for Digital, Culture, Media & Sport (2017), *Summary of GDPR derogations in the Data Protection Bill*, August 2017.

HM government Department for Digital, Culture, Media & Sport (2018), *Data Protection Bill Factsheet – Overview*, March 2018.

House of Commons Business Innovation and Skills Committee (2016), *The Digital Economy*, Second Report of Session 2016-17.

Information Commissioner's Office (2016), *Data Protection Act 1998 Supervisory Powers of the Information Commissioner Monetary Penalty Notice to TalkTalk Telecom Group PLC*, September 2016.

Woodhouse, J. & Lang, A. (2017), *Briefing Paper: Brexit and data protection*, October 2017, House of Commons Library, London.

Websites

Autoriteit Persoonsgegevens, accessed 27/01/2018 https://autoriteitpersoonsgegevens.nl/en/about-cbp/mission-vission-and-core-values.

https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens, accessed 07/02/2018.

https://autoriteitpersoonsgegevens.nl/en/about-dutch-dpa/commissioners-dutch-dpa, accessed 03/03/2018.

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf , accessed 15/03/2018.

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_in_een_notendop.pdf , accessed 15/03/2018.

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg#over-welke-onderwerpen-geven-de-europese-privacytoezichthouders-uitleg-in-guidelines-6189 , accessed 15/03/2018.

Baker & McKenzie (2016), *2016 Global Data Protection Enforcement Report*, accessed 25/03/2018, https://iapp.org/media/pdf/resource_center/BM-2016-Global-Enforcement-Report.pdf

Information Commissioner's Office, 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 09/02/2018.

https://ico.org.uk/about-the-ico/who-we-are/management-board/, accessed 03/03/2018.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/, accessed 03/03/2018.

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf ,accessed 02/03/2018.

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/ , accessed 03/03/2018.