Ministry of Justice

Review of the Balance of Competences

Call for Evidence on the Review of the Balance of Competences between the United Kingdom and the European Union

Information Rights

Date of publication: 27 March 2014

Closing date for evidence: 01 July 2014

Contents

Chapter I: Introduction to the Balance of Competences Review

Introduction

1. The Foreign Secretary launched the Balance of Competences Review in Parliament on 12 July 2012. This takes forward the Coalition commitment to examine the balance of competences between the UK and the European Union (EU). The review will provide an analysis of what the UK's membership of the EU means for the UK national interest. It will not be tasked with producing specific recommendations or looking at alternative models for Britain's overall relationship with the EU.

2. Instead, it aims to deepen public and Parliamentary understanding of the nature of our EU membership. It also aims to provide a constructive and serious contribution to the national and wider European debate about modernising, reforming, and improving the EU in the face of collective challenges.

3. The overall review will be broken down into a series of reports on specific areas of EU competence, spread over four semesters between autumn 2012 and autumn 2014. The review is led by the Government but will also involve non-governmental experts, organisations, and other individuals who wish to feed in their views. Foreign governments, including our EU partners and the EU institutions, are invited to contribute. The process will be comprehensive, evidence-based, and analytical. The progress of the review will be transparent, including in respect of the contributions submitted to it.

What is competence?

4. For the purposes of this review, we are using a broad definition of competence. Put simply, competence in this context is about everything deriving from EU law that affects what happens in the UK. That means examining all the areas where the Treaties give the EU competence to act. This includes the provisions in the Treaties giving the EU institutions the power to legislate, to adopt non-legislative acts, or to take any other sort of action. It also means examining areas where the Treaties apply directly to the Member States without needing any further action by the EU institutions.

5. The EU's competences are set out in the EU Treaties. These provide the basis for any actions the EU institutions take. The EU can only act within the limits of the competences conferred on it by the Treaties, and where the Treaties do not confer competences on the EU, they remain with the Member States.

6. There are different types of competence: exclusive, shared and supporting. In areas where the EU has exclusive competence, only it can act. Example

7. When exercising competence, the EU must act in accordance with fundamental rights (such as freedom of expression and non-discrimination) as set out in the Charter of Fundamental Rights. It must also act in accordance with the principles of subsidiarity and proportionality. Under the principle of subsidiarity, if the EU does not have exclusive competence, it can only act if it is better placed than the Member States to do so because of the scale or effects of the proposed action. Under the principle of proportionality, the content and form of EU action must not exceed what is necessary to achieve the objectives of the EU treaties.

Scope of this Review

8. This review will explore the development of EU competence in the field of Information Rights, how that competence has been exercised up to the present day, and also possible future developments. Taking its lead from the key rights that now appear in the EU Treaties, the review will focus on data protection rights and the right to access official information.

9. The Treaty on European Union states, in Article 4.2, that national security remains the sole responsibility of each Member State. Therefore, this review does not propose to examine information rights in the national security context. Data sharing for police and criminal justice purposes is being dealt with in the Police and Criminal Justice Review in Semester 4.

10. This review is UK wide, and we therefore encourage contributions from stakeholders across the UK, including Scotland, Wales, and Northern Ireland.

Interdependencies with other Reviews

11. There are several potential topics where EU competence may affect both information rights and other areas under review by the Government as part of this Balance of Competence exercise. Findings and evidence from our review will be shared with other government departments as appropriate.

12. While we value responses on any area that affects information rights, you may be interested in other reviews that relate directly to this review:

    - **Police and Criminal Justice** (Semester 4)

    - **Voting, Consular and Statistics** (Semester 4): the collection and publication of statistics will be covered under the Cross-cutting Report.

13. Further details and how you can contribute evidence to these reviews can be found on the balance of competences review web page at: https://www.gov.uk/review-of-the-balance-of-competences.

A brief history of the EU treaties

The Treaty on the European Economic Community (EEC) was signed in Rome on 25 March 1957, along with the Treaty establishing the European Atomic Energy Community (EURATOM). It entered into force on 1 January 1958. The EEC Treaty had a number of economic objectives, including establishing a European common market.

Since 1957, there has been a series of treaties extending the objectives of what is now the European Union beyond the economic sphere. The amending treaties (with the dates on which they came into force) are:

- the Single European Act (1 July 1987), which provided for the completion of the single market by 1992;
- the Treaty on European Union (1 November 1993) - the Maastricht Treaty - which covered matters such as justice and home affairs, foreign and security policy, and economic and monetary union;
- the Treaty of Amsterdam (1 May 1999), the Treaty of Nice (1 February 2003), and the Treaty of Lisbon (1 December 2009), which made a number of changes to the institutional structure of the EU.

Following these changes, there are now two main treaties which together set out the competences of the European Union:

- The Treaty on European Union (TEU); and
- The Treaty on the Functioning of the European Union (TFEU).

What are Information Rights?

The "word cloud" above provides an indication of significant terms generally associated with information rights. It is important to note that there is no settled official meaning for the term "information rights". The concept is not recognised in the EU Treaties and has no particular significance in EU or domestic law.

So in this review, we will use the term "information rights" to signify two key rights that are now specifically given by the Treaty on the Functioning of the European Union (TFEU).

These are:

- The right of individuals to have their **personal data** protected when it is used within the EU or sent from within the EU to a country outside it. This is found in Article 16(1) TFEU; and

- The right of EU residents to access **official documents** in the possession of the main EU institutions. This is found in Article 15(3) TFEU.

Other rights that generally have a much wider focus but may sometimes apply when information is being used or shared, such as the right to a private life and family life, are not within the scope of this Review.

The Development of EU Competence

Data Protection

14. Data Protection has a long history in the UK. Many domestic and international rules providing for the protection of personal data predate action taken on the EU level by a decade or more.

The UK Dimension

15. In the UK, it has long been established that personal information should be protected in certain contexts. We expect doctors to protect confidential information about their patients, and lawyers about their clients. Principles such as these existed long before any law dedicated to data protection was passed.

16. We can trace the development of legislation in this area back to at least 1970 and the establishment of the Younger Committee[1]. This Committee conducted a survey about public attitudes to privacy. More and more personal information was beginning to be held on computer systems, and the survey indicated people's fears were growing about what their data would be used for and who could access it.

17. In the meantime, certain protections began to be provided in consumer law regarding the use of personal data for decisions about creditworthiness. The Consumer Credit Act of 1974 allowed individuals to access information held about them by credit reference agencies and, if necessary, amend it. In the fields of healthcare and education, similar rights of access to information were created in statute.

18. In 1976, the Lindop Committee[2] was established and charged with exploring what could be done to improve the protection of personal data. The Committee reported in 1978 and recommended the creation of an independent body that would draw up statutory codes of conduct for various sectors, both private and public.

19. The UK also took note of important international developments which were happening at the same time. The passing of the Data Protection Act 1984 (the background to which is explained in more detail below) is evidence of this.

[1] In 1970 the UK Government appointed Kenneth Younger to chair a Committee on Privacy which reported in 1972.
[2] In July 1975, the UK Government announced the setting up of a Data Protection Committee under the Chairmanship of Sir Norman Lindop

The International Dimension

20. Many developments in the 20th century led some countries to adopt data protection measures. This was in part in response to the growing use of computers to store and process personal data, which meant rules were needed to protect it from being stolen or disclosed to those without authorisation.

21. Personal data also needed to be kept accurate: many automatic decisions were being taken that had an impact on people, such as those concerning pensions, insurance, or creditworthiness. As more and more countries enacted data protection legislation, fears grew in some quarters that these measures would stifle the flow of data that was becoming increasingly important for international trade.

22. In 1980, the Organization for Economic Cooperation and Development (OECD) issued a set of guidelines for how personal data should be protected. The OECD stated that its member countries have a common interest in protecting both personal data and the global free flow of information.

23. In 1981, the Council of Europe introduced a new international binding agreement on data protection, which is commonly known as Convention 108[3]. The aim of this Convention is to reconcile data protection with the free flow of information. Focusing on the automatic processing of personal data, it set out many key principles that remain central to data protection law today. These include the principles that personal data be processed fairly and lawfully, that it be processed only for specific purposes, and that it be accurate and kept up to date. It established rights of access to personal data, rights to rectify and erase personal data, and it also designated authorities who could cooperate to ensure the protection of personal data across borders.

24. The Convention's, general principles were incorporated into the Data Protection Act 1984. This established in UK law the rights for individuals to have access to data that was held about them and to correct any inaccuracies.

The EU Dimension: what is the competence and how did it develop?

25. During a similar time-frame, EU law[4] had also begun to move towards recognising data protection rights. The original Treaties establishing the EU did not provide specific data protection rights. However, the Court of Justice of the European Union (the CJEU) recognised that establishing a free market would inevitably result in more and more personal data being shared between

[3] The UK signed Convention in 108 in 1981 and ratified in 1987

[4] Note references to the EU in this paper also encompass the Union under its previous titles (e.g European Economic Community.

companies and across borders. Protecting this data against misuse was vital to ensure that free market measures enjoyed the confidence of the individuals whose data was being shared. For this reason, a right to data protection was, over time, recognised by the CJEU as a fundamental right. Further detail on the CJEU case law in this area is contained in the Legal Annex.

26. However, it remained the case throughout the 1970s and 1980s that, even after it was first recognised that there may be data protection rights in EU law, the EU had not asserted competence to pass legislation on the subject. Partly as a consequence of this, the European Commission recommended that Member States ratify Convention 108 to bolster rights in this area. However, by 1990, almost half of all Member States had not yet done so. Amongst those who had ratified it, there were believed to be wide differences in its implementation.

27. This caused concern that a lack of confidence in data protection standards might, in effect, create new trade barriers within the developing single market. Some Member States also worried that their own national measures would be redundant if personal data had to be transferred to another state with lower or non-existent safeguards.

28. The first step towards harmonisation of data protection rules by the EU was taken in 1990, when a draft Data Protection Directive was proposed by the Commission. This was the first time the EU asserted competence to legislate in the area of data protection, and it did so using the development of the single market as its legal base[5]. The provisions of the agreed Directive are examined in more detail in Chapter 2 below.

29. The exercise of competence has had a significant effect on the way that data is protected throughout the Member States of the EU. Despite its origins as a single market measure, the CJEU has found that the Directive can apply even where use of data in a particular case has no link to the operation of the free market.

30. The EU's competence regarding data protection has been put on a formal footing by the inclusion of Article 16 in the TFEU. That gives a specific right to data protection (in Article 16(1)) and gives the EU competence via a dedicated Treaty provision (in Article 16(2)) to pass legislation which supports that right.

31. This competence, while extensive is not exclusive: it is shared with Member States. Either the Member States or the EU may act, but when the EU has acted first, Member States cannot do so afterwards in a way that would conflict with what the EU has done. When the EU acts, all decisions must be taken jointly by the European Parliament, and the Council, which represents

[5] Article 100a of the Treaty Establishing the European Community.

the governments of all Member States. The CJEU will interpret EU legislation when a case has been brought before it. Its judgments are binding on all Member States.

32. Additionally, the EU's legislative competence under Article 16 cannot be used to:

- regulate activities which are outside the scope of EU law;
- regulate activities that are subject to EU rules that the UK has opted out of (e.g. on police or judicial co-operation between Member States in criminal cases);
- regulate processing of personal data in the context of common foreign and security policy (this has its own legal base under Article 39 TFEU);
- make legislation that is incompatible with Article 8 of the Charter on Fundamental Rights[6].

These restrictions are discussed in more detail in the Legal Annex.

How the EU has exercised competence in data protection

33. The first (and still the most significant) exercise of EU competence to make legislation about data protection is the Data Protection Directive[7]. The Directive has a broad scope and provides a general data protection framework to be implemented by each Member State through its own national legislation.

34. It took five years from publication of the original proposal until the text was finally agreed. It expands on Convention 108 and was transposed into UK law through the Data Protection Act 1998 (DPA 1998).[8] This Act replaces and extends the data protection regime created by the 1984 Act.

35. It remains the key piece of EU legislation when considering how personal data may be used within the EU. Accordingly, it is described in greater detail in Chapter 2 and forms the main focus of how this review will examine how

[6] Article 8 of the Charter of Fundamental Rights states that everyone has the right to the protection of personal data concerning him or her.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[8] For more information on the Data Protection Act 1998, please see http://www.legislation.gov.uk/ukpga/1998/29/contents

EU competence has impacted on the UK in the field of data protection.

36. However, in order to give the full picture, it is necessary to describe briefly the other legislation that has resulted from the exercise of EU competence in this area.

37. In 2001, the EU passed Regulation (EC) No 45/2001. This effectively applies the same rules contained in the Data Protection Directive to the EU institutions themselves when using personal data in the course of EU business. Without this Regulation, those rules would not apply to the EU institutions as the Directive does to the EU's various Member States.

38. In 2002, the EU introduced the E-Privacy Directive[9], which imposes a number of obligations on data controllers, particularly in areas such as online marketing or when cookies[10] and spam[11] are used. The Directive's aim was to strengthen privacy in the light of new digital technology and its spread. Directive 2009/136 later updated this and obliged controllers to gain the individual's consent before using cookies to collect and process their data.

39. The UK implemented both instruments via the Privacy and Electronic Communications Regulations 2003 (PECR). PECR sets out various obligations and rules that govern organisations' use of marketing through electronic means, including nuisance calls and spam. Organisations must gain the consent of users before tracking them online.

40. In 2008, a Framework Decision (the DPFD[12]) made specific provision for the protection for personal data in cases where that data was used for the cross-border police or judicial co-operation purposes in criminal matters. A framework decision is a type of EU legislation that does not have direct effect. The DPFD currently applies to the UK.

41. The Legal Annex describes how the UK retains a right not to be bound by certain police or judicial co-operation measures at EU level, including the DPFD.

42. So far as policing is concerned, the DPFD does not impact on the use of personal data for purely national purposes; instead, it only covers personal

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[10] Text files placed on a user's computer by a website or online service. They contain information such as the website's name and a unique code assigned to the computer. When the user revisits the website, it will check to see if this cookie exists and process the information contained in it. The website may tailor the content it provides based on that information.

[11] Unsolicited messages sent over the internet, typically to large numbers of users, for the purposes of advertising, phishing etc

[12] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML

data which is shared between police in one Member State and police in another. For example, if the Metropolitan Police sent data to the Greater Manchester Police, the DPFD would not apply. However, if the data were sent to a police force in France, it would.

43. The DPFD is therefore not always applicable but where it is, it uses the same definitions as the Data Protection Directive and provides for broadly similar rights and obligations, with some differences. For example, 'to make anonymous' is defined as being to modify personal data in such as way that details of personal or material circumstances can no longer, or only with disproportionate investment of time, cost and labour, be attributed to an identified or identifiable person'. Guidance was provided to organisation and others on how to apply the DPFD through a circular[13] issued by the Ministry of Justice in 2011. That circular, along with the domestic provisions in the DPA, serves to implement the DPFD in the UK. Given the broad similarities between the DFPD and the Data Protection Directive, it is not proposed to examine the DPFD in detail in this call for evidence.

EU Proposals

44. In the last few years, the European Commission has argued for the need to bring the Data Protection Directive up to date in light of challenges posed by new technological developments, the growth of targeted advertising on the internet, and increased sharing of personal data online. The Commission has also highlighted the lack of harmonisation persisting after the Data Protection Directive's entry into force. EU action in this area remains focused on the single market, and the emerging Digital Single Market in particular. The Commission has argued that the fragmented nature of the data protection framework across the EU was costly for businesses across borders as policies had to be adapted to the domestic legislation for each Member State.

45. On 25 January 2012, the European Commission published new legislative proposals for data protection on the basis of the specific legal base given by Article 16(2). The proposals contain both a Regulation (for processing generally) and a Directive (for processing in police and judical co-operation cases, even where there is no cross-border element). However, the internal processing of police data will not be regulated by the Directive as far as the UK is concerned[14].

46. To increase harmonisation, the Commission has chosen a Regulation as the

[13] Circular 2011/01: www.justice.gov.uk/downloads/legislation/bills-acts/circulars/moj/data-protection-framework-decision-circular.pdf

[14] That is because Article 6a of Protocol 21 enables the UK to limit the scope of data protection measures in the field of police and judicial cooperation in criminal matters. EU data protection rules only apply in this field where the UK is bound by an EU measure which provides for the sharing of data. Further detail is included in the Legal Annex.

instrument to repeal and replace the Data Protection Directive. Unlike a Directive, the provisions in Regulations are directly applicable to all Member States. A Regulation can impose binding legal obligations and create enforceable rights for the individual without the need for primary national legislation.

47. The UK Government recognises that there is a need to update the EU data protection legislation to ensure it remains effective for both individuals and business. Effective harmonisation of laws across Member States is important, but there should be sufficient flexibility within the proposals to allow businesses (including large multinational corporations, small and medium enterprises, and sole traders) to innovate and grow. The protection of individuals' privacy and the pursuit of economic growth should not be attained at the expense of one or the other.

48. The potential impact on the digital marketing and internet advertising industries, which contribute to the growth of the UK economy, is a particular issue. Many of these businesses rely on the collection data such as IP addresses and 'cookies'. Where this data allows individuals to be treated differently from others (e.g. through personalised advertising), then, even if it doesn't give their name, the data protection rules may apply.

49. The Regulation as proposed by the Commission therefore affects the collection of this type of data and may impact negatively on these industries. This is because some of the new obligations proposed in the Regulation would potentially be very onerous when applied to this sort of data.

50. As well as re-stating and in some cases, revising, rights and obligations which appear in the current Directive, the Commission's proposed Regulation creates both new rights for data subjects and obligations on data controllers. These include:

- a 'right to be forgotten'; meaning that the data subject has the right to request that the controller erase all personal data held about them and where the data has been passed to a third party, steps are taken to ensure that copies of the data or links to it are also erased to. The proposed right to be forgotten is an extension from the 1995 Directive;

- a new right for the individual to receive a copy of their electronic data in a format they can easily use and transfer to another system;

- an obligation to appoint a data protection officer. Organisations with at least 250 employees would have to employ a data protection officer if they regularly process personal data;

- an obligation on data controllers to inform the regulatory authority of a data breach within 24 hours; and

- an expanded terrotiorial scope. The proposed Regulation would extend to controllers outside the EU when they process EU residents' personal data.

51. The Commission's proposed Directive would apply to "competent authorities" processing personal data for criminal justice purposes. It would repeal and replace the DPFD 2008. It aims to extend the DPFD to cover internal processing of personal data.

52. The UK Government published its own impact assessment of the proposed Regulation in 2012, in response to the European Commission's impact assessment. Although the UK concluded that there are benefits to be gained from the reduction in legal fragmentation, there would also be a high cost to business of implementing the proposed administrative and compliance measures. The UK impact assessment estimated that the costs of meeting the requirements of the Commission's original proposals to UK small businesses would be between £80-£290 million per annum.

Access to Official Information

Activity on the EU level: Official Information (non-Environmental)

53. In the run up to the Maastrict treaty, there was concern expressed about the EU's transparency. For this reason, this Treaty led to the EU Commission and Council working together to improve public access to information of the main EU institutions.

54. The result was a Code of Conduct, which was adopted formally and came into force in 1994[15]. This created a right of access to Council and Commission documents, subject to exceptions and a right of review if requests were refused.

55. Building on this, Article 255 of the 1995 Treaty of Amsterdam provided a specific right of access to official documents of EU institutions for EU residents. It also provided the Council with a power to set out general principles and limits to the right in further legislation. The EU then used this power to pass the Access to Public Documents Regulation[16] in 2001.

56. The Regulation allowed EU residents to view documents of the main EU institutions. It only applies to documents held or written by an EU institution. This can include documents created by the UK which have been sent to an EU institution and are in its possession. However, it does not affect UK official documents that are only in the possession of the UK Government.

57. The EU's competence in this area has been preserved by Article 15 of the TFEU following the negotiation of the Treaty of Lisbon.

Activity on the UK Level

58. These developments have not affected the ability of the UK to decide whether to make its own arrangements for accessing official information. Accordingly, the Westminster and Scottish Governments each considered that it was important to increase the accountability of Government and to encourage public participation in policy making. This led to the Freedom of Information Act 2000 (FOIA) in England, Wales, and Northern Ireland, creating legal rights to access official information of listed public bodies in the UK. Freedom of Information is a devolved matter in Scotland and is legislated for there under the Freedom of Information Act (Scotland) 2002.

59. FOIA applies to more than 100,000 bodies in England, Wales, and Northern Ireland. It gives a general right of access to any recorded information held by bodies subject to the Act. It requires that any written request is answered

[15] See Decisions 93/731 and 94/90.
[16] Regulation (EC) No. 1049/2001.

within 20 working days.

60. Where a request requires consideration of the public interest balance, the statutory time limit for responding can be extended. It does not, however, apply to requests for environmental information or one's own personal data which are considered under the EU-derived rules relating to data protection and, in respect of environmental information, the arrangements described in the section immediately below.

61. The objectives of FOIA were: increased openness and transparency, more accountable government, better decision-making and increased public participation in decision-making. FOIA has played an important role in increasing openness and transparency, resulting in the release of significant amounts of information that may otherwise have gone undisclosed. FOIA has also enabled more accountability by revealing decisions, policies or processes for which public authorities have had to account to individuals or the media.

Environmental Information

62. Both the European Commission and the United Nations Economic Commission for Europe (UNECE)[17] came to consider that increasing public concerns about the impact of human activity on the environment and the emergence of an information society required a more proactive approach to dissemination of material using the latest technologies.

63. Accordingly, Council Directive 90/313/EEC on the freedom of access to information on the environment required public authorities to make available information relating to the environment on request. In 1998, the United Nations adopted the Aarhus Convention[18], which granted individuals the right to access environmental information from public authorities. This was ratified by the EU and the UK.

64. In 2003, the EU agreed Directive 2003/4[19] on public access to environmental information, which has its origins in the Aarhus Convention. The Directive applies to official environmental information held by public authorities in all Member States, and was transposed into UK law by the Environmental Information Regulations 2004 (the EIRS) and the Environmental Information (Scotland) Regulations 2004. Although an earlier Directive[20] existed, this was

[17] The UNECE was established in 1947 to encourage economic cooperation among its member states

[18] UNCE Convention on Access to Information , Public Participation in Decision-making and Access to Justice in Environmental Matters, signed 25 June 1998, entered into force 30 October 2001

[19] Directive 2003/4/EC on Public Access to Environmental Information has its legal basis in the treaty of the European community and in particular article 175(1).

[20] Directive 90/313/EEC

the first time the EU explicitly set out the legal right to access environmental information. Until then, although it was possible to obtain environmental information, there was no such right to the information.

65. The EIRs apply to the majority of public authorities that are subject to FOIA and some additional bodies. They create a number of obligations for public authorities and private bodies performing certain public functions. The main principles are that access to information on environmental matters will:

- encourage greater awareness of issues that affect the environment;
- contribute to more effective public participation in decision–making;
- increase accountability and the transparency of public bodies' actions;
- recognise the need to protect, preserve and improve the state of the environment;
- build public confidence and trust in those actions;

66. The EIRs provide a general right of access to recorded environmental information, which includes information about air, water, soil, land, plants animals, energy, noise, waste and emissions such as pollution and radiation. Environmental information also includes information about decisions, policies, and activities that affect the environment or protect the environment.

Re-use of Public Sector Information

67. Directive 2003/98/EC was introduced by the European Commission to facilitate the re-use of public sector information. Unlike the Access to Documents Regulation or FOIA this does not give a free-standing or enforceable right of access to information. Instead, where certain types of information are provided by a public authority (either on a voluntary basis or in response to a request for it under a formal access regime such as FOIA) it says that the information should be provided in reusable form.

68. Its broad aims were to increase the availability of official information to the public by removing barriers across Member States, and to promote its re-use, including for commercial purposes. The Commission envisaged this could generate savings, innovations, and job creation. The Commission also intended to improve evidence-based policy across the EU by ensuring a wider availability of public data.

69. The Re-use of Public Sector Information Regulations 2005 implemented this Directive into UK law, where it is one of many initiatives supporting re-use of information as part of the Government's Transparency Agenda. A revision to 2003/98/EC was adopted by the EU in June 2013 (2013/37/EU) extending re-use to be mandatory in some circumstances. Transposition is in progress and has to be completed by July 2015.

Chapter II: Information Rights – Data Protection

Introduction

70. This chapter will examine in more detail how the EU's has used its competence in data protection by looking more closely at the Data Protection Directive. In this field, the impact of EU policy for the UK can be grouped under four key headings. These are:

- Rights – EU policy aims to give data subjects more rights and control over their personal information held by others.
- Obligations – EU policy places certain obligations and restrictions on those holding and using the personal information. This Review will look at the effect this has on businesses and other organisations.
- Regulatory Bodies – EU policy affects the powers and practices of the UK's Information Rights regulatory body, the Information Commissioner's Office (ICO).
- International – EU policy shapes the ways organisations can transfer personal data internationally.

Some common data protection concepts

71. **Personal data** means any information that can identify a living individual. It can include your name, address, and date of birth. It can also extend to information about purchases you have made, your health history, even your library records.

72. People who decide how this information is used and what it is used for are called **data controllers**. Controllers can be other individuals (but not when using data for household or personal purposes), private companies, charities, local councils, government departments, police forces: that is anyone who makes decisions about how your personal data is used. A **data processor** is a person or body that processes personal data on behalf of the data controller but does not make the key decisions.

73. Under the Data Protection Directive individuals have certain rights about how their personal data are used by others who hold it. However, data protection rules do not always apply For example, the scope of the Data Protection Directive does not extend to individuals processing personal data in the course of a purely personal or household activity. This is commonly referred to as the **"household exemption**".

Malcolm wants to keep records about his family and friends to help him with his Christmas card list. He creates a database on his computer and stores their names, addresses, and other relevant information in it. This counts as a "personal or domestic" activity, and Malcolm would not be subject to the Directive.

Data Protection Rights

74. EU information rights policy aims to give more rights to individuals in relation to the storage and use of their personal data by others. In the UK, the rights contained in the Data Protection Directive have been transposed into domestic law through the DPA 1998[21]. They include a right to access the information held about them; a right to object to it being processed; a right to object to having decisions taken based on automated processing; a right to rectify inaccurate data or have it erased; and a right to claim compensation for breaches of these rights.

Right to Access

75. The Data Protection Directive grants each individual the right to access their personal data. In practical terms, this means a person is entitled to be informed of details such as whether personal data are being processed about them, why it is being processed, and whether it has been sent to anyone else. Individuals are also entitled to request a permanent copy of data held about them. The Directive permits controllers to charge a fee for this. The UK has set this fee at £10 as a maximum for most cases. Under the UK's implementation of the Directive there are strictly limited grounds for refusing to provide a copy of the information. These include where certain exemptions set out in the DPA apply or when providing copies of the personal data in permanent form would require disproportionate effort.

Right to Object to Processing

76. The Data Protection Directive sets out a person's right to object to their data being processed in certain situations. When the data are used for direct marketing purposes, the controller must comply with any request to cease processing. .

77. For all other purposes, processing has to cause unwarranted and substantial damage or distress before the controller has to comply with an objection. This allows data to be processed where there is a good justification for doing so even if it causes damage to the individual - for example, information

[21] For more information on the Data Protection Act 1998, please see www.legislation.gov.uk/ukpga/1998/29/contents

leading to their arrest.

78. There is potential for overlap between the ePrivacy Directive and PECR on the one hand, and the Data Protection Directive and the DPA 1998 on the other hand. When an organisation is conducting direct marketing by phone or online, it is usually subject to PECR. However, when the marketing involves an individual's personal data, the DPA 1998 takes precedence.

After going on a package holiday, Jo receives unsolicited emails from the travel firm advertising their latest promotional offers. She asks the travel firm to stop sending these emails. The firm has 28 days to comply.

Right not to be subject to Automated Processing Decisions

79. This right refers to decisions about a person taken wholly by automated means (such as by a computer) based on their personal data. The Data Protection Directive gives that person the right to object to such decisions if they would have legal effects or otherwise significantly affect them. Examples of such decisions could involve automated assessments of a person's creditworthiness and predictions of future behaviour.

80. The Directive provides exemptions allowing the controller to refuse to comply, including when they need to perform this processing for a contractual or legal obligation and have safeguards in place.

When Amish applied for his loan online, it was refused automatically. He realised the decision relied on a computer algorithm which processed his personal data. He asks the loan provider to have an employee review the decision. The loan provider cannot rely on a contractual or legal exemption and so agrees to Jack’s request for human intervention.

Right to Rectification or Erasure

81. The Data Protective Directive gives an individual the right to ask a controller to rectify any incomplete or inaccurate data, or have it erased.

Gemma has applied for a mortgage but is refused. She later finds out that her credit report linked her with a wrong address. Gemma contacts the credit reference agency and asks them to correct the address information. If the agency does not comply, Gemma can refer the matter to a court. The court may then order the agency to correct or delete the incorrect data or add a supplementary statement to Gemma's file detailing what is being disputed.

Right to Compensation

82. Individuals may suffer damage due to processing which breaches the Data Protection Directive. The Directive, obliges Member States to provide a means for people to receive compensation when the controller is found to be at fault.

Obligations

83. Data Protection rights are reinforced by corresponding obligations of controllers to guarantee the rights already mentioned. In addition to those obligations, EU policy places further responsibilities on controllers. These include the obligation to have lawful grounds for processing and to respect sensitive data in particular. They also include the obligations to be transparent about processing, to disclose personal data in a fair manner, and to have appropriate security measures.

Grounds for Processing

Article 6 of the Data Protection Directive 95/46/EC sets out the Principles Relating to Data Quality

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

84. The Data Protection Directive provides that processing can only take place if it is based on one or more grounds specified in the Directive. The grounds include where the individual's consent has been obtained, where the processing is necessary to comply with legal or contractual obligations, or where it is necessary in order to pursue a goal in the public interest.. Any consent from a person must be “unambiguous.” This obligation and others are transposed into the DPA 1998 through the Principles[22].

85. The Directive requires controllers to satisfy themselves that one or more of the specific grounds listed above applies when they wish to process personal data. To gather “sensitive personal data” about a person, an organisation must draw on an additional ground to justify this. These grounds are also specified in the Directive.

86. Sensitive personal data may consist of information on areas such as a person's ethnicity, health, sexual preferences, and political or religious beliefs. When the controller relies on a person's consent to process such sensitive information, the consent must be “explicit”. However, consent is not the only ground which can be relied on to processing this sort of data.

A fitness website offers personalized exercise plans based on information provided by its customers about their health and lifestyle. It also uses the information to track its popularity amongst different demographics. Information about a person's health is considered sensitive data. The website will need its customers' explicit consent to both of these processing activities.

87. The Directive also accords some flexibility to Member States to use their national law to exempt controllers from the requirement to identify a ground for processing sensitive personal data. The exemptions can only apply in certain areas detailed in the Directive, including public health and social protection.

Information to the Individual

88. The Data Protection Directive places an obligation on the controller to tell a person when their data are being processed. They must also inform them of their rights (including the right to receive a copy of the paper in permanent form), the purposes for the processing, and of any intention to disclose the data to others. Processing must be fair, and this requires transparency.

[22] The Data Protection Act 1998’s Principles: www.legislation.gov.uk/ukpga/1998/29/schedule/1

Amanda signs up for a supermarket loyalty card. The supermarket intend to record information about the items she buys using the card and process it so they can send her advertisements for certain products. The supermarket must inform Amanda of this when she signs up.

Disclosure to third parties

89. The Data Protection Directive gives Member States the broad flexibility to determine when organisations can disclose personal data to others, providing it is fair and lawful.

A bank keeps a record of its customers' financial activity. Whenever the bank finds suspicious transactions that may indicate money laundering, it discloses the relevant personal data to HMRC. This disclosure would be deemed fair and lawful, as the bank has a legal obligation to report its suspicion.

Regulatory Bodies

90. The Data Protection Directive requires that each Member State sets up an independent supervisory body. This body is charged with monitoring the compliance of organisations and public authorities with data protection law. The Directive obliges Member States to give the supervisory authority powers to investigate complaints, to compel organisations to stop processing, and to hand out sanctions or to take them to court in the event of breaches of the law. The Directive gives Member States the discretion to decide what form these sanctions will take.

91. The Data Protection Framework Decision also obliges member states to set up a supervisory authority with similar powers to regulate public law enforcement or judicial bodies processing data. However, it asks Member States to ensure the supervisory authority's power does not interfere with the independence of the judiciary and police.

92. In the UK, the supervisory authority is the Information Commissioner's Office (ICO)[23]. The DPA 1998 requires the ICO to advise organisations and individuals about how to comply with data protection law and to regulate this compliance with the legislative framework. The ICO has a number of powers. These include: criminal prosecution, non-criminal enforcement, and audit. The ICO may also serve a monetary penalty notice on a data controller for

[23] The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest

breach of the DPA.

European Data Protection Supervisor and Article 29 Data Protection Working Party

93. The European Data Protection Supervisor (EDPS) monitors how the EU institutions process personal data. The EDPS has no powers to make binding decisions or recommendations. Instead, it offers advice and works with other regulators such as the ICO to ensure consistent protection of personal data across the EU. The EDPS is appointed through co-decision by the European Parliament and the Council, after the Commission has drawn up a shortlist of candidates. The EDPS will then serve a five year term.

94. The Article 29 Working Party is composed of the EDPS, representatives from each Member State's regulatory body, and representatives from the Commission and other EU institutions. The Working Party may issue opinions on the implementation of the Data Protection Directive, particularly in light of new practices or technological developments. For example an opinion has been issued on mobile apps and a decision was issued on the use of binding corporate rules. These opinions have the status of non-binding advice and guidance: Member States retain the primary responsibility to implement the Directive.

International Data Transfers

95. International data flows are numerous, complex, and diverse. They are also vital to the global economy, and as e-commerce develops, they will continue to increase in importance. Data flows are regulated by a number of framework agreements at an international level. The way EU data protection laws interact with third countries also has an impact. The aim of the relevant provisions in the Data Protection Directive on cross border flows of personal data is to ensure that personal data transferred outside the European Economic Area (EEA) is handled in accordance with the key data protection principles.

Data Sharing between the EU/EEA and Third Countries

96. Many countries outside of the EU have different standards in relation to the protection of personal data or different legislative frameworks. The Data Protection Directive prohibits the transfer of data outside the EEA unless the recipient country has adequate level of personal data protection, or an exemption (the Directive calls them “derogations”) permitted by the Directive and provided for in Member State law applies.

Adequacy Findings

97. An “adequacy decision” is a decision adopted by the European Commission which establishes that a third country ensures an adequate level of protection of personal data by reason of its domestic law or the international commitments it has entered into. The effect of such a decision is that personal data can flow from the 28 EU Member States and the three European Economic Area member countries to that third country, provided that any flow of this sort complies with all other relevant aspects of the Data Protection Directive.

98. Adequacy decisions are normally adopted after a number of formal steps have been taken; these include a proposal from the Commission; an Opinion of the Article 29 Working Party; an opinion of the Article 31 Committee[24] delivered by a qualified majority of Member States; a thirty-day right of scrutiny for the European Parliament to check if the Commission has used its executing powers correctly; and the adoption of the decision by the College of Commissioners.

99. Since 1995, only a small number of countries or territories have been deemed adequate by the Commission. These are: Andorra, Argentina, Canada, Switzerland, the Faroe Islands, Guernsey, the State of Israel, Isle of Man, Jersey, New Zealand, and Uruguay. Partial adequacy findings have been made for the United States to regulate the transfer of Passenger Name Record information[25]. A similar agreement exists with Australia's Customs Service.

EU-US Safe Harbor

100. Safe Harbor is an agreement between the EU and the US under which participating US organisations are recognised as providing an adequate level of data protection pursuant to the ’95 Directive. This recognition is achieved by compliance with the relevant Safe Harbor Principles. The US Department of Commerce maintains a public list of participating companies, and each firm must verify their continuing compliance on an annual basis to remain on the list.

101. In November 2013, the Commission published a Review [26] on the protection that Safe Harbor offers to data subjects. The Review contained 13 recommendations that focused on the areas, such as a need for more

[24] A special committee of Member States that the EU Commission can convene to discuss particular aspects of the Data Protection Directive, for example the agreement of adequacy decisions

[25] EU-US PNR Agreement http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:215:0005:0014:EN:PDF

[26] http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

transparency and enforcement. The Commission is looking to conclude an agreement with the US Government on reforming Safe Harbor by summer 2014.

102. The United State's approach to the protection of personal data is different from the EU's approach. In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead the US has a number of statutory protections, which are specific to sectors or particular problems, for example the Children's Online Privacy Protection Act 1998. The regime also relies on self-regulatory mechanisms, for example guidelines developed by governmental agencies and industry groups which are not legally enforceable but are considered best practice. This is very different from the EU approach of aiming to provide harmonised rules across Member States.

Member States

103. The Data Protection Directive also allows Member States acting on an individual basis to authorise transfers to countries without an adequacy finding if the controller has applied adequate safeguards to the data, such as contractual clauses that govern how the data will be handled by the recipient.

Exemptions

104. In addition to the above, the Data Protection Directive permits Member States to apply certain exemptions that allow a person’s data to be transferred to countries without an adequacy finding. In these circumstances, the controller has the responsibility of assessing the transfer and does not need to submit it for prior approval. The derogations set out in Article 26(1) of the Directive are:

- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject; or

- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Cloud Computing
More and more data processing is taking place through Cloud Computing. This is when data are stored on remote computers and accessed through a network. Cloud computing offers organisations lower costs, greater economies of scale, and faster information and service delivery.

In September 2012 the European Commission published a strategy entitled *Unleashing the Potential of Cloud Computing in Europe*. The EU believes that it is possible for an extra EUR 45 billion to be spent on developing Cloud Computing in the EU by 2020, creating 3.8 million more jobs. The EU also works with stakeholders through the European Cloud Partnership to review how to smooth the pathway ahead for this goal. There are no clear geographical borders within the Cloud. This may pose a challenge to data protection rules that govern international transfers.

Chapter III: Rights of Access to Official Information

Introduction

105. Information Rights include not only your right to control your own data, but also to access certain official information. The principal piece of EU legislation in this area is the Regulation 1049/2001[27] ("the Public Access to Documents Regulation") that allows access to documents of the EU institutions. This chapter will set out the rights afforded by this Regulation and its corresponding obligations and exemptions.

106. This chapter will also look at the Environmental Information Directive (2003/4/EC) and the Re-use of Information Directive (2003/98/EC). Although they are not based on Article 15(3) of the TFEU, both provide rights of access to information. The UK Freedom of Information Act is also relevant as an example of the UK exercising competence in the information rights policy area.

Public Access to Documents

Rights

107. The Public Access to Documents Regulation regulates the right of EU residents to access EU documents. The right itself is enshrined in Article 15(3) of the Treaty on the Functioning of the European Union and reflected in the EU Charter of Fundamental Rights.

108. A key conceptual difference between this and the right created by the UK's Freedom of Information Act is that the right created by the Public Access to Documents Regulation is limited to official documents, rather than official information. The EU right was initially limited to documents held by the three main EU institutions: the Commission, the Council, and the Parliament. Various subsequent provisions outside the Public Access to Documents Regulation have applied it to other EU institutions. Individuals have the right to appeal any decision.

Obligations

109. Article 15(3) and the Public Access to Documents Regulation places obligations on the EU agencies and bodies to release documents held or authored by the Commission, the Parliament, or the Council upon request. EU institutions must also maintain a publicly available register of documents. This obligation may be waived in certain circumstances. The possible exemptions fall into two categories: relative exceptions and absolute exceptions. Unless there is an overriding public interest in disclosure, relative

[27] Regulation 1049/2001 http://www.europarl.europa.eu/RegData/PDF/r1049_en.pdf

exceptions may be invoked when disclosure would undermine the protection of:

- commercial interests, including intellectual property;
- court proceedings and legal advice;
- inspections, investigations, and audits;
- the decision-making process.

110. Before relying on these exceptions, the EU institution must weigh the benefits to society of disclosing the document against the harm it could cause to the protection of one of the above issues.

111. Absolute exceptions may be invoked if disclosure would undermine the protection of:

- public security;
- defence and military matters;
- international relations;
- the financial or economic policy of a Member State or the EU;
- the privacy and integrity of the individual.

112. The EU institutions may invoke these absolute exceptions without performing a public interest test. The EU agencies and bodies have the obligation to interpret these exceptions narrowly and provide the justification for any decision to withhold the document.

Elisabeth is a student in France carrying out research into the development of EU agriculture policy. Under the Access to Documents Regulation, she requests documents held by the European Commission.

The Commission considers her request and notices that some of documents contain personal data from third parties. They provide her with the majority of the information she asked for, with the personal data removed in accordance with the exception for such material in the Regulation.

113. The Access to Public Documents Regulation does not provide a right to request information directly from UK authorities. However, if an EU institution covered by the Regulation has been given documents by the UK then a request can be made under the Regulation for a copy of those documents. The position is different where an EU document has been sent to a member State. A request for that will usually be dealt with under any relevant domestic legislation. In the UK, any such request would be dealt with under the UK, Freedom of Information Act 2000 or its Scottish equivalent. In such cases, the Regulation requires the Member States to consult with the EU institution concerned, unless it is clear that the document should or should not be released.

Oliver requests information under the UK's Freedom of Information Act about immigration policy. The official who handles his request notices that documents originating from the Council of the European Union are relevant to it. It is not immediately clear whether these should be disclosed. The official consults the Council about disclosure in accordance with the Access to Documents Regulation. The Council agrees to disclose the documents.

Sensitive Documents

114. Documents classified as "sensitive" do not have to be added to the published register, but they may be added with the consent of the originator. The Regulation uses classifications to define sensitivity, such as "Secret" or "Restricted", instead of the exceptions above. However, a classification of "sensitive" may indicate that an exception may well apply.

Environmental Information Regulations (EIRs)

Rights

115. The EIRs provide individuals with a right of access to environmental information held by or for public authorities. Public authorities will include some private-sector bodies which are performing public functions. Individuals who make a request under the EIRs have the right to do so verbally or in writing. They do not have to provide a reason for their request.

Obligations

116. The EIRs impose a duty on public authorities to disseminate information about their activities relating to or affecting the environment and to make information available on request. Public authorities are obliged to respond to requests for information within twenty working days in general, or forty at most if the information is complex or voluminous. They are obliged to disclose the information unless there is a public interest argument in favour of maintaining a relevant exception. The EIRs apply a presumption in favour of disclosure. An authority may withhold information when disclosure would harm the public interest, but such grounds should only be used in restricted circumstances. When an authority refuses a request, they must justify their decision to the applicant.

117. Additional obligations on public authorities include the requirement to proactively disseminate environmental information and to assist the public in seeking access to information. There are also procedures for the review of the acts or omissions of public authorities, in particular before a court of law.

CHAPTER IV: Call for Evidence

How to Respond

We are requesting input from anyone with relevant knowledge, expertise, or experience. We would welcome contributions from individuals, companies, civil society organisations including think-tanks, and governments or government bodies. We welcome input from those within the UK, or beyond our borders. This is your opportunity to express your views.

Your evidence should be objective and factual information about the impact EU competence has had in your area of expertise. We will expect to publish your response and the name of your organisation, unless you ask us not to (but please note that even if you ask us to keep your contribution confidential, we might have to release it in response to a request under the Freedom of Information Act). We will not publish your own name unless you wish it to be included.

Please base your responses on the questions set out below.

Please send your evidence to balanceofcompetences@justice.gsi.gov.uk by 01 July 2014. The contact point for related enquiries is informationrightsboc@justice.gsi.gov.uk.

Engagement/Workshops

The Ministry of Justice will be hosting a number of discussion events in London (29 April), Edinburgh (28 May) and Brussels (June tbc). These events are free to attend although places will be limited.

Questions

1. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

2. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals' data protection rights and the pursuit of economic growth?

3. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?

4. What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

5. What evidence is there that the right to access documents of the EU institutions has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

6. How would UK citizens' ability to access official information benefit from more or less EU action?

7. How could action, in respect of information rights, be taken differently at national, regional or international level and what would be the advantages and disadvantages to the UK?

8. Is there any evidence of information rights being used indirectly to expand the competence of the EU? If so, is this advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

9. What is the impact on EU competence of creating an entirely new legal base for making data protection legislation that is not expressly linked to the EU's single market objectives?

10. What future challenges or opportunities in respect of Information Rights might be relevant at a UK, EU or international level; for example cloud computing?

11. Is there any other evidence in the field of EU Information Rights that is relevant to this review?

Legal Annex – Description of Competence

Pre-Lisbon

Data Protection

1. Specific EU competence in the area of data protection is a relatively recent development. A Treaty right to data protection and associated legislative competence was only explicitly provided for following the revision of TFEU by the Treaty of Lisbon, which came into effect in 2009.

2. The original Treaties of 1952 and 1957, which established the European Communities, were silent on whether EU law guaranteed minimum rights for individuals in the field of data protection. Instead, the original Treaty provisions gave the EU express competence to legislate in order to establish a single market.

3. However, the Court of Justice of the European Union (CJEU) increasingly recognised the importance of safeguarding rights and of ensuring individuals were offered minimum guarantees in respect of those rights in all Member States. This became seen as an integral part of creating a fully effective single market that enjoyed the trust of those who participate in it.

4. In the course of giving effect to such rights, the CJEU recognised that the right to protection of personal information is a **general principle** of EU law.[28]

5. General principles are part of the EU's primary law, which is binding on the EU and its Member States.[29] This means that the EU and, in certain circumstances, its Member States, must comply with the general principles. Having recognised the right to protection of personal information, the CJEU has taken it into account when interpreting and ruling on the validity of acts of the EU and its Member States.

6. Consistent with these developments, the EU asserted competence to legislate in the field of data protection for the first time in 1990.

7. The legal base for proposing legislation (which led to the 1995 Directive) was the then 100a of the Treaty Establishing the European Community. Accordingly, the EU's competence to legislate on data protection, prior to the coming into force of the Lisbon Treaty, was an expression of its competence to take appropriate measures to encourage the free

[28] Case 26/69 Stauder, [1969] ECR 419.
[29] Cases C-402/05 and C-415/05 P Kadi, judgment of 3 September 2008.

movement of goods and services within the EU.

8. To that extent, the EU's ability to legislate took effect subject to the wider limitations on its competence. Accordingly, the 1995 Directive could have no effect in areas (for example, national security) that the EU did not have competence to act in.

9. That said, and despite its status as a free market measure, subsequent CJEU case law made it clear that, in its view, there did not need to be a specific link to free movement in order for the Directive to apply in a given situation[30].

Post-Lisbon

10. Following the amendments made by the Lisbon Treaty, the EU has explicitly been given competence to act on data protection as a subject in and of itself, through Article 16 of the TFEU.

11. Article 16(1) provides each individual whose personal data is processed within the EU (regardless of nationality or place of residence) with a right to protection of their personal data.

12. Article 16(2) then empowers the Council and Parliament to make rules about the use (or "processing") of personal data by Union institutions or Member States, when either are *"carrying out activities which fall within the scope of Union law."*

13. Any rules made using this power are subject to the ordinary legislative procedure. This means there is qualified majority voting in the Council, which must come to a co-decision with the European Parliament.

14. However, the EU's competence in making data protection rules under Article 16(2) is limited. Some of these limits are specific to the UK and a small number of other Member States. There are four key limitations.

15. The first limitation is that rules can only be made to regulate EU institutions or Member States when they are carrying our activities "*within the scope of EU law*" i.e. activities that relate to something that the EU can legislate on more generally.

16. This limitation also affects the issue of shared competence. There may be activities that fall within an area that the EU *could* legislate on but has yet to do so. The UK considers that such activities are **not** carried out "within the scope of EU law". Therefore, data protection rules could not be made under Article 16(2) to regulate the use of personal data for those activities

[30] See *Osterreichischer Rundfunk* [2003] ECR 1-000 and *Lindqvist* C-101/01.

or areas.

17. On competence and matters of national security, Declaration 20 annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon recognised that whenever rules laid down on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. The conference recalled that the legislation presently applicable (in particular the 1995 Data Protection Directive) contains specific derogations on these subjects.

18. Article 346(1)(a) TFEU is also significant. It provides that no Member State is obliged to disclose information if it considers that disclosure would be contrary to its essential security interests.

19. The second limitation is contained in Article 6a of Protocol 21 to the EU Treaties on the position of the UK and Ireland in respect of the area of freedom, security, and justice (Protocol 21 annexed to the TFEU). The EU's power to make rules governing activities in this area are set out under Title V of TFEU. Generally speaking, Protocol 21 allows the UK to "opt into" Title V rules. If the UK does not opt into those rules in this way, then they will not apply.

20. Rules passed under Title V powers may include those concerning police or judicial cooperation between Member States in criminal cases involving the interests of more than one Member State. Activity authorised by those rules might require Member States to share personal data. Normally, data protection rules under Article 16(2) would apply to govern how the personal data are used in such instances.

21. However, Article 6a of Protocol 21 states that if the UK is not opted into police and judicial cooperation rules, then more general EU data protection rules that would ordinarily apply to that activity will not apply either. In brief, this means that if the UK does not opt into police and judicial cooperation rules, the UK retains competence to make its own rules on those topics and may apply its own data protection standards accordingly.

22. The third limitation is that Article 16(2) of TFEU does not cover the protection of personal data in the context of common foreign and security policies. Rules for such areas should be made under Article 39 of TFEU. This states that it is for the Council to adopt a decision laying down rules when carrying out activities that fall within the scope of common foreign and security policy, and rules relating to the free movement of such information. To date, no measures have been made under Article 39.

23. The final limitation is that any exercise of competence by the EU under Article 16 must comply with article 8 of the Charter of Fundamental Rights, which, following the Lisbon Treaty, enshrines existing rights.

24. Article 8 provides a right to the protection of personal data. This might appear to duplicate the right given by Article 16(1). However, it would be possible for the EU to breach the Charter right if it were to enact legislation under Article 16(2) that failed properly to give adequate protection to personal data.

25. In giving effect to the Article 8 right, the CJEU has held that the right reflects the **fundamental right** to respect for private life in Article 8 of the European Convention on Human Rights, and the right to protection of personal data. These were both already part of EU law before the Lisbon Treaty came into force.[31]

26. The CJEU has shown that it is willing to examine EU legislation closely and critically in light of the Article 8 right.

27. For example, in the case of *Volker*[32] the Court held that EU Council regulations[33] were incompatible with Article 8 of the Charter to the extent that they required the publication of the names of all people in receipt of funding from the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development.

28. By way of contrast in *Schwarz*[34], the Court considered it was compatible with Article 8 of the Charter for a Regulation to require that when people applied for passports, their fingerprint data should be collected and stored. The requirements were a proportionate means of protecting against the fraudulent use of passports.

Access to Official Information

29. High levels of public disinterest or even distrust of the EU had been noted in the lead-up to the negotiation of the Maastricht Treaty. For this reason Declaration 17 annexed to that Treaty recommended that the EU

[31] In cases C-92/09 and C-93/09 *Volker* [2020] ECR I-11063 paragraphs 76-77, the CJEU interprets the right in Article 8 of the Charter by reference to pre-Lisbon case law such as Case C-73/07 *Satakunnan* [2008] ECR I-9831. In case C-104/10 *Kelly*, judgment of 21 July 2011, paragraph 55, after referring to EU acts such as Directive 95/46/EC, the Court says, "The protection of personal data is also provided for in Article 8 of the Charter of Fundamental Rights of the European Union". In case C-291/12 *Schwarz*, judgment of 17 October 2013 at paragraph 27, it refers to case law of the Strasbourg Corut when considering the concept of personal data for the purpose of Article 8.
[32] Cases C-92/09 and C-93/09.
[33] Article 44a of Regulation 1290/2005.
[34] Case C-291/12.

Commission and Council work together to improve public access to information of the main EU institutions. This was inspired partially by a wish to regain this lost public confidence and interest through transparency and greater accountability.

30. The result was a Code of Conduct, which was adopted formally and came into force in 1994[35], on public access to Commission and Council documents. This created a right of access to Council and Commission documents, subject to exceptions and a right of review if documents were refused. There were subsequent disputes in EU court proceedings about the correct legal basis for the Code of Conduct and whether it was right for the access arrangements to be limited to Council and Commission documents.

31. Article 255 of the 1995 Treaty of Amsterdam provided a specific right of access to official documents of EU institutions for EU residents. It also provided the Council with a power to set out general principles and limits to the right in further legislation. The Article 255 Right and legal base have since been replicated and replaced by Article 15(3) of the TFEU during the negotiation of the Treaty of Lisbon.

32. Article 15(3) of TFEU now gives EU residents a right of access to documents held by the EU's main institutions, bodies, offices, and agencies. That Article also provides that the European Parliament and the Council may establish general principles and limits on how the right may be used. These should be set out in a Regulation, passed using ordinary legislative procedure.

33. The UK retains exclusive competence to pass legislation relating to access by the public to information held by public authorities in the course of their duties.

Environmental Information

34. In 1984 the UK's Royal Commission on Environmental Pollution recommended that there should be a presumption in favour of unrestricted access for the public to information which the pollution control authorities obtain or receive by virtue of their statutory powers. In line with the formulation recommended by the Royal Commission, the government proposed a resolution during the UK Presidency of the European Community in 1986 calling for access to environmental information to be made available throughout the Community. In 1987 the Council of the European Communities passed a resolution to this effect.

[35] See Decisions 93/731 and 94/90.

35. The direct result of the 1987 resolution was Council Directive 90/313, which was followed by the UK legislation implementing that Directive in 1992. For the first time the public had a statutory right of access to environmental information held by public authorities.

36. A succession of UN-inspired agreements led to similar conclusions, starting with the first United Nations conference on the environment in Stockholm in 1972, which decided that traditional and contemporary mass communications media should be used to disseminate information. Twenty years later the Rio conference agreed a new set of principles, recognising that citizens should be involved in environmental issues, through having access to information held by public authorities.

37. At a regional level the UNECE sponsored the Aarhus Convention in 1998, granting the public rights and imposing on public authorities obligations regarding access to information, public participation in decision-making and access to justice.

38. Aarhus was implemented at EU level by the repeal and replacement of the original Environmental Information Directive in February 2003. The new Directive was transposed by the UK Environmental Information Regulations 2004, which came into force on 1 January 2005.

39. The UK, as a Member State, retains competence to take whatever necessary legislative measures are required in order to ensure compliance with the obligations in the Directive. Whilst the Directive sets out the general framework of the right of access to environmental information it leaves to the Members States the task of defining the practical arrangements under which information is effectively made available to the public.