

OBLIGATIONS IMPOSED ON PRIVATE PARTIES BY THE GDPR AND UK DATA PROTECTION LAW: BLURRING THE PUBLIC-PRIVATE DIVIDE

OLIVER BUTLER¹

ABSTRACT

A profound shift across European public law has occurred as public authorities and private actors are increasingly interconnected in the exercise of public functions. This article explains the differences between the obligations imposed on private parties and public authorities by the European Union General Data Protection Regulation and UK Data Protection Bill, which is currently before the UK Parliament. It considers whether such a divide is justifiable, especially in light of private parties increasingly performing public functions, and makes recommendations for the interpretation and development of the public-private divide in the future. Although the structure adopted in the UK Data Protection Bill has the ability to achieve a coherent and appropriate public-private divide, it will present a considerable administrative challenge and must be monitored closely in the future.

KEY WORDS

Data Protection; GDPR; Private Actors; Public Authorities; Public Functions; Privacy; Information.

1. INTRODUCTION: PUBLIC AUTHORITIES AND PRIVATE ACTORS IN DATA PROTECTION

A profound shift across European public law has occurred as public authorities and private actors are increasingly interconnected in the exercise of public functions. The historic divide between public and private sectors is under unprecedented strain from a variety of sources, including privatization, contracting out and governance by contract.² Complex flows of personal data are crucial to sustaining these processes. The flow of data does little to respect the distinction between public authorities and private actors.³ As the distinction between public authorities and private actors is blurred, and data is both required to flow and to be protected, this raises the question of whether and how far the law regulating data protection should recognize distinctions between public authorities and private actors. This is especially so where private actors are involved in the performance of public functions.

In the context of the European Convention on Human Rights (ECHR) and the UK Human Rights Act 1998, Palmer has argued that the traditional public-private divide has been 'blurred' through 'privatisation, outsourcing and projects under the Private Finance Initiative (PFI)'.⁴ She argues that this is a 'serious threat to public law values' and human rights in the 'exercise of power by private or quasi-public institutions'.⁵ Public and private have become 'inextricably linked owing to the radical changes to our social structure and institutions,' including 'an increase in the role of the private, voluntary and charitable sectors in the provision of public services'.⁶ This article explores the effect of this trend on European and UK data protection

¹ Fellow of Wadham College, Oxford and Associate Research Fellow of the Bonavero Institute of Human Rights. Email: oliver.butler@wadham.ox.ac.uk. I am grateful to Carlo Colombo and Mariolina Eliantonio for comments on a draft of this paper. Any errors are my own.

² Peter Vincent-Jones, *The Regulation of Contractualisation in Quasi-Markets for Public Services* Public Law 304 (1999).

³ Neil Richards, *The Dangers of Surveillance* 126 Harvard Law Review 1934 (2012-2013).

⁴ Stephanie Palmer, *Public, Private and the Human Rights Act 1998: an Ideological Divide* CLJ 559, 559 (2007).

⁵ *Ibid.*, 559 to 560.

⁶ *Ibid.*, 561.

law. How well do the categories and paradigms adopted in data protection address the problems created by a blurring of the public-private divide?

Peter Blume argues that a basic issue in the EU General Data Protection Regulation (GDPR) is whether public and private sectors should be subject to the same rules.⁷ He argues that an 'essential' question for data protection is whether a 'systematic division' is required.⁸ For Blume, whereas traditional human rights have regulated the relationship between the individual and the state as 'negative rights',⁹ data protection is important as a 'primary and in some sense vanguard example of the broad application of human rights'.¹⁰

This article explains the differences between the obligations imposed on private parties and public authorities by the GDPR and UK Data Protection Bill, which is currently before the UK Parliament. It considers whether such a divide is justifiable, especially in light of private parties increasingly performing public functions, and makes recommendations for the interpretation and development of the public-private divide in the future. Although the structure adopted in the UK Data Protection Bill has the ability to achieve a coherent and appropriate public-private divide, it will present a considerable administrative challenge and must be monitored closely in the future.

2. THE OBLIGATIONS IMPOSED ON PRIVATE PARTIES AND PUBLIC AUTHORITIES IN THE GDPR

2.1. The grounds for lawful data processing

The GDPR comes into force from 25th May 2018.¹¹ It has a legal basis in Article 16 TFEU, which provides that 'everyone has the right to the protection of personal data concerning them'.¹² Article 16(2) TFEU provides for 'rules relating to the protection of individuals with regard to the processing of personal data... by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data'. It subjects compliance with those rules to the control of independent data protection authorities.¹³

The Recitals to the GDPR show some awareness of the challenges presented by the increased participation of public and private actors in co-operation and in the co-exercise of public functions. The Recitals observe that the 'exchange of personal data between public and private actors... across the Union has increased'¹⁴ and 'technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities'.¹⁵

Provision is made in the GDPR to regulate lawful processing by both private actors and public authorities. In this regard, Article 6(1) GDPR sets out six potential grounds for lawful processing:

- a. processing with the consent of the data subject;¹⁶
- b. processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;¹⁷

⁷ Peter Blume, *The Public Sector and the forthcoming EU Data Protection Regulation*, EDPL 32, 32 (2015).

⁸ *Ibid.*, 32.

⁹ Peter Blume, *Data Protection in the Private Sector*, 47 Scandinavian Stud. L. 297, 298 (2004).

¹⁰ *Ibid.*

¹¹ Art. 99(2) GDPR.

¹² Art. 16(1) TFEU.

¹³ Art. 16(2) TFEU.

¹⁴ Recital 5 GDPR.

¹⁵ Recital 6 GDPR.

¹⁶ Art. 6(1)(a) GDPR.

¹⁷ Art. 6(1)(b) GDPR.

- c. processing necessary for compliance with a legal obligation to which the controller is subject;¹⁸
- d. processing necessary in order to protect the vital interests of the data subject or of another natural person;¹⁹
- e. processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;²⁰ and
- f. processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party.²¹

Many of these grounds contain no differences in their application to public authorities or private actors. Article 6(1)(c) GDPR, *compliance with a legal obligation*, and Article 6(1)(e) GDPR, *processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*, are the most obvious grounds for public authorities to rely upon. However, these grounds are also relevant for private actors where legislation imposes legal obligations on them, makes them responsible for public tasks, or vests them with official authority. Recital 45 GDPR explains that it is for the Union or Member State law in question to determine whether a data controller performing the tasks in Article 6(1)(e) GDPR 'should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so... by private law'.²² This part of the GDPR is therefore designed to be of equal application to either public authorities or private actors, enabling data protection to regulate data processing across the public-private divide, where that data processing relates to public functions.

Similarly, sometimes a public authority will enter into a *contract* with data subjects and process according to Article 6(1)(b) GDPR. Therefore, this ground is also of equal application to both private parties and public authorities.

Both public authorities and private controllers might also process data where this is *necessary to protect the vital interests of the data subject or another natural person* under Article 6(1)(d) GDPR. There is accordingly no public-private divide regarding processing pursuant to this ground.

Neither does Article 6(1)(a) GDPR, *consent of the data subject*, have a public-private divide on its face. However, consent must be, among other things, 'freely given'.²³ On whether consent is freely given, Recital 43 GDPR explains that 'consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation'. Certainly, it is true that in other circumstances consent may not in fact be 'freely given' and therefore the full significance of Recital 43 GDPR for the public-private divide might be limited. For example, Article 7(4) GDPR requires the assessment of whether consent is freely given to take 'utmost account' of 'whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data not necessary for the performance of the contract'. However, Recital 43 GDPR certainly suggests a belief that the phenomenon is more likely to occur, or the problem more acute, in the context of public authorities. The divide is unlikely to make a significant difference in practice, however, as the extent to which consent is 'freely

¹⁸ Art. 6(1)(c) GDPR.

¹⁹ Art. 6(1)(d) GDPR.

²⁰ Art. 6(1)(e) GDPR.

²¹ Art. 6(1)(f) GDPR: 'except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

²² Recital 45 GDPR.

²³ Art. 4(11) GDPR.

given' in the context of public functions will be similar irrespective of whether it is performed by a public authority or private body.

The most significant difference, on the other hand, between the obligations of public authorities and private parties relates to Article 6(1)(f) GDPR, *processing necessary for purposes of the legitimate interests pursued by the controller or a third party*. Legitimate interests may not be relied upon by 'public authorities in the performance of their tasks'.²⁴ The Recitals explain that this is because 'it is for the legislator to provide by law for the legal basis for public authorities to process personal data' and therefore legitimate interests should not be relied upon for 'processing by public authorities, in the performance of their tasks'.²⁵

Article 6(1)(f) establishes that legitimate interests can be relied upon as a ground for lawful data processing by private actors. This might appear to be the case even where the private actors could alternatively rely on Article 6(1)(c) or (e). This gives rise to a problem of *election by private actors*. That is, a private actor might be placed in a position whereby the actor can elect to rely on their legitimate interests or rely on Article 6(1)(c) or (e). It could be therefore that the involvement of private actors in data processing in the context of public functions could undermine the insistence in Article 6(3) GDPR that processing under Article 6(1)(c) or (e) must be laid down in either Union law or Member State law to which the controller is subject. This requirement is important because it subjects data processing necessary for a legal obligation, the performance of a task in the public interest or in the exercise of official duty to Union or national law and therefore to legality and a greater possibility of democratic oversight and transparency. The potential of Article 6(3) GDPR to limit data processing in this way would be reduced where a private party exercising public functions relies on legitimate interests processing instead.

A related question arises as to the proper definition of hybrid bodies which have a mixture of public and private functions. These are not straightforwardly public authorities or private actors. What does a 'public authority in the performance of its tasks' mean in such cases? One possibility is that this refers to all the tasks of a public authority: the *institutional view*. This view is binary at the institutional level: a body is either a public authority and can never rely on legitimate interests or it is not a public authority and can rely on legitimate interests. The merit of the view is to reflect that public authorities cannot pursue independent legitimate interests but only act according to law. This view leads to the difficult question of which 'hybrid' bodies are public authorities for the purposes of the GDPR and which are private actors. It enforces a strict institutional separation between public and private institutions.

Another possibility is that 'the performance of its tasks' is a qualifier so that it only applies to public authorities in the performance of its tasks *qua* public authority. Where a public authority also has private functions, those functions are not its functions as a public authority and legitimate interests processing remains available. This appears plausible: if public authorities were not able to rely on legitimate interests at all, then Article 6(1) GDPR could omit the wording 'in the performance of its tasks'. This might be characterized as an *institutional and functional view*. Institutions must be defined as public authority or private actor but the limitation on legitimate interests processing only applies to the *public functions* of *public authorities*. A broad categorization of hybrid bodies as public authorities is then less problematic because only the tasks of a 'public authority' that are public functions are unable to rely on legitimate interest processing. Although this would mitigate some problems of the public-private divide, the problem of election still remains in relation to private actors. Which may elect to rely on legitimate interest processing when involved in the exercise of public functions. A broad categorization of hybrid bodies as public authorities combined with the institutional and functional view of this provision is, however, preferable in light of the blurring

²⁴ Art. 6(1) GDPR.

²⁵ Recital 47 GDPR.

of the public-private divide in the exercise of public functions. It is personal data processing for the performance of public functions for which the legislator should provide by law.

2.2. Other differences between the obligations of private actors and public authorities

Some provisions of the GDPR treat processing in reliance on Article 6(1)(c) or (e) more favourably than processing on other grounds. These avoid some problems from the blurring of the public-private divide that are not avoided by other parts of the GDPR because those grounds are equally available to public authorities or private actors.

For example, the right to erasure in Article 17 GDPR gives data subjects the 'right to obtain from the controller the erasure of personal data concerning him or her without undue delay', where certain conditions apply. This right does not apply to the extent that the processing is necessary for processing for compliance with a legal obligation, in the performance of tasks in the public interest or for the exercise of official authority.²⁶ It is questionable whether such processing should be given blanket protection from the right to erasure, for example which applies to erasure where the data have been unlawfully processed.²⁷ However, it applies equally to such processing, which may be carried out by public authorities or private actors. As such, it does not create problems where private actors exercise public functions and rely on Article 6(1)(c) or (e) as a ground for processing.

However, if private actors are able to elect legitimate interests processing when contracted to deliver public services, the right to erasure could be used by individuals, whereas the same processing would not be subject to a right to erasure if carried out directly by a public authority in the performance of a task in the public interest. This does have some capacity to introduce arbitrary distinctions.

Article 55(2) GDPR provides that 'where processing is carried out by public authorities or private bodies', in reliance on Article 6(1)(c) or (e), then 'the supervisory authority of the Member State concerned shall be competent'. Otherwise, the data controller may be subject to a lead supervisory authority in another Member State.²⁸ Again this provision does not depend on whether a public authority or private actor is performing public functions.

There are several provisions in the GDPR which, however, contain significant differences between the obligations of public authorities and private parties. Their significance lies in the potential to introduce arbitrary and undesirable distinctions in circumstances where both public authorities and private controllers interact in the delivery of public functions. In the context of the public-private divide in human rights law, some have argued that the fact that protections for individual could vary 'according to the method of service delivery',²⁹ causing 'inequality'³⁰ or the loss of a remedy against the public authority,³¹ as well as potentially discriminating between publicly privately funded recipients of public services, is unjust.³² Similar considerations arise here and support a broad interpretation of public authority.

One difference between public authorities and private actors concerns the obligation to appoint a data protection officer. Data protection officers must be designated in any case where 'processing is carried out by a public authority or body, except for courts acting in their judicial capacity'³³ but only otherwise where the 'core activities' of the controller or the processor of

²⁶ Art. 17(3)(b) GDPR.

²⁷ Art. 17(1)(d) GDPR.

²⁸ Art. 56 GDPR.

²⁹ Paul Craig, *Contracting out, the Human Rights Act and the Scope of Judicial Review*, 118 LQR 551, 554 (2002).

³⁰ Catherine Donnelly, *Leonard Cheshire again and beyond: private contractors, contract and s.6(3)(b) of the Human Rights Act*, PL 785, 788 (2005).

³¹ *Ibid.*

³² *Ibid.*, 790.

³³ Art. 37(1)(a) GDPR.

personal data consist of either an 'operation which... require[s] regular and systematic monitoring of data subjects on a large scale'³⁴ or 'processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10'.³⁵ Recital 97 GDPR explains that data protection officers are persons with 'expert knowledge of data protection law and practices' who 'assist the controller or processor to monitor internal compliance' with the GDPR. It is striking that all public authorities, however limited the data processing carried out, must have a data protection officer, whereas only private actors participating in certain types of processing activity are similarly required. It is not obvious why the professionalization and present of data protection officers is more important in public authorities than in private parties, especially in cases where the latter exercise public functions.

A public-private divide also exists regarding enforcement. The monitoring of approved codes of conduct does not apply to processing carried out by public authorities and bodies.³⁶ The option to bring proceedings 'before the courts of the Member State where the data subject has his or her habitual residence' is not available where the 'controller or processor is a public authority of a Member State acting in the exercise of its public powers'.³⁷ Where 'the controller is a public authority of a Member State acting in the exercise of its public powers' proceedings can only be brought in the courts of the Member States where it has an establishment.³⁸ Typically, this is the Member State of the public authority. Where the controller is a private party, such proceedings can also be brought in the data subjects' Member State of residence.³⁹

Therefore, where public authorities and private actors co-exercise functions, participate cooperatively in the provision of services or engage in mixed markets of public service provision, strange anomalies may occur regarding a private actors' exposure to litigation in other Member States. As this will often have the effect of complicating the litigation and increasing the costs for the controller, one might wonder whether this will, in effect, encourage private actors to settle claims on less favourable terms or concede points to the data subject to avoid litigation which a public authority, unexposed to such risks, may be left in a position to resist.

Finally, Article 83(7) GDPR provides that 'each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies in that Member State'. Recital 150 GDPR explains that it 'should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines'. In Member States where this opportunity is taken, differences in exposure to financial risk resulting from breach of the GDPR could be very significant, with a serious potential to distort relationships between public authorities and private actors engaged in the performance of public functions.

A public authority is therefore protected from enforcement outside the Member State and may be exempt from administrative fines, although it is subject to broader obligations to have a data protection officer. Private actors do not enjoy these privileges but when performing public functions might be able to rely on legitimate interests processing to a greater extent than public authorities and are required to appoint data protection officers only in more limited circumstances. They therefore enjoy greater flexibility in innovative data processing to support its tasks but are more exposed to enforcement action. These differences in the GDPR could be problematic where private actors exercise public functions by introducing arbitrary or

³⁴ Art. 37(1)(b) GDPR.

³⁵ Art. 37(1)(c) GDPR.

³⁶ Art. 41(6) GDPR.

³⁷ Art. 79(2) GDPR.

³⁸ Recital 145 GDPR.

³⁹ Recital 145 GDPR.

undesirable distinctions. It would be desirable to include private actors performing public functions in the definition of public authorities to avoid such arbitrary distinctions.

3. THE PUBLIC-PRIVATE DIVIDE AND THE UK DATA PROTECTION BILL

The UK Parliament is currently considering a Data Protection Bill, which implements parts of the GDPR. The original Bill adopted an *institutional and functional* approach to defining public authorities, creating a definition capable of treating private actors exercising public functions or carrying out public functions under contract in the same way as public authorities. However, an amendment at Report Stage altered this approach by introducing a *purely functional view* of public authorities. This has important implications for the public-private divide in UK data protection law.

The Data Protection Bill defines the meaning of 'public authority' and 'public body' in clause 7 by reference to the UK freedom of information legislation definitions of 'public authority' in the Freedom of Information Act 2000⁴⁰ and 'Scottish public authority' in the Freedom of Information (Scotland) Act 2002.⁴¹ For the purposes of the GDPR these definitions apply and are supplemented by a power of the Secretary of State to specify further authorities or bodies by regulations,⁴² subject to the affirmative resolution procedure in Parliament.⁴³ Those regulations can provide that a person that is a public authority under the freedom of information legislation is 'not a "public authority" or "public body" for the purposes of the GDPR'.⁴⁴ These definitions are therefore only a starting point, subject to amendment by secondary legislation. There will therefore be a list of 'public authorities' for the purpose of the GDPR. This has important implications for the definition of hybrid bodies and private bodies that also exercise public functions.

The definition of 'public authorities' and 'Scottish public authorities' are considerably complex. The Freedom of Information Act 2000 in turn defines a 'public authority' by reference to a list of persons and office holders in Schedule 1 to the 2000 Act,⁴⁵ those designated by order under section 5,⁴⁶ or those which are a 'publicly-owned company' under section 6.⁴⁷ The Freedom of Information (Scotland) Act 2002 defines 'Scottish public authorities' in the same way in Schedule to the 2002 Act,⁴⁸ by designation orders,⁴⁹ or as a publicly-owned company.⁵⁰

Schedule 1 to the 2000 Act can be amended by the Secretary of State or the Minister for the Cabinet Office by order,⁵¹ including specified persons or offices by description,⁵² where two conditions are met. The first is that the body is 'established by virtue of [Crown prerogative] or by an enactment or by subordinate legislation' or 'in any other way by a Minister of the Crown in his capacity as Minister, by a government department or by the Welsh Ministers, the First Minister for Wales or the Counsel General to the Welsh Government'.⁵³ The second is that, concerning bodies, 'the body is wholly or partly constituted by appointment made by the Crown, by a Minister of the Crown, by a government department or by the Welsh Ministers, the First Minister for Wales or the Counsel General to the Welsh Government' and, concerning

⁴⁰ Data Protection Bill (As amended on Report), cl. 7(1)(a).

⁴¹ *Ibid.*, cl. 7(1)(b).

⁴² *Ibid.*, cl. 7(1)(c).

⁴³ *Ibid.*, cl. 7(4).

⁴⁴ *Ibid.*, cl. 7(3).

⁴⁵ Freedom of Information Act 2000, s. 3(1)(a)(i).

⁴⁶ *Ibid.*, s. 3(1)(a)(ii).

⁴⁷ *Ibid.*, s. 3(1)(b).

⁴⁸ Freedom of Information (Scotland) Act 2002, s. 3(1)(a)(i).

⁴⁹ *Ibid.*, s. 3(1)(a)(ii).

⁵⁰ *Ibid.*, s. 3(1)(b).

⁵¹ Freedom of Information Act 2000, s. 4(1).

⁵² *Ibid.*, s. 4(6).

⁵³ *Ibid.*, s. 4(2) (as amended).

offices, 'appointments are made' by those same bodies.⁵⁴ Where those conditions subsequently cease to exist, the 'body or holder of that office shall cease to be a public authority by virtue of the entry' on the Schedule to the Act.⁵⁵ There is a power to remove such entries and entries in relation to bodies which have ceased to exist by order.⁵⁶ No orders can be made under section 4 or section 5 in relation to the Scottish Parliament, any part of the Scottish Administration, the Scottish Parliamentary Corporate Body or any Scottish public authority with mixed functions or no reserved functions within the meaning of the Scotland Act 1998.⁵⁷ These are addressed by the 2002 Act. The Scottish Ministers may amend Schedule 1 to the 2002 Act by order adding or removing bodies or office holders, specific or by description,⁵⁸ who are 'part of the Scottish Administration or a Scottish public authority with mixed functions or no reserved functions'.⁵⁹

The designation powers allow private actors to be included within the definition of 'public authority' where they exercise 'functions of a public nature' or are carrying out functions of public authorities under contract. The Secretary of State or the Minister for the Cabinet Office of bodies may designate bodies by order, relating to a specific person or office or by description of them,⁶⁰ where they are not listed in, or capable of addition to, Schedule 1 to the 2000 Act, and where the body 'appears to the [relevant Minister] to exercise functions of a public nature'⁶¹ or 'is providing under a contract made by a public authority any service whose provision is a function of that authority'.⁶² Two such designation orders have been made under the 2000 Act.⁶³ The Scottish Ministers may designate persons under the 2002 Act, specific or by description,⁶⁴ as a 'Scottish public authority' who 'appear to the Scottish Ministers to exercise functions of a public nature'⁶⁵ or 'are providing, under a contract made with a Scottish public authority, any service whose provision is a function of that authority'.⁶⁶ They may not designate bodies that could be added to Schedule 1 to the 2002 Act or other public bodies or office holders.⁶⁷ Scottish designation orders must specify the functions of a public nature or service being provided.⁶⁸ Two designation orders have been made under the 2002 Act.⁶⁹

⁵⁴ *Ibid.*, s. 4(3) (as amended).

⁵⁵ *Ibid.*, s. 4(4).

⁵⁶ *Ibid.*, s. 4(5).

⁵⁷ *Ibid.*, s. 80.

⁵⁸ Freedom of Information (Scotland) Act 2002, s. 4(3).

⁵⁹ *Ibid.*, s. 4(1).

⁶⁰ Freedom of Information Act 2000, s. 5(2).

⁶¹ *Ibid.*, s. 5(1)(a).

⁶² *Ibid.*, s. 5(1)(b).

⁶³ Freedom of Information (Designation as Public Authorities) Order 2011 designated, for certain of their functions, the Association of Chief Police Officers of England, Wales and Northern Ireland, the Financial Ombudsman Service, and the Universities and Colleges Admissions Service as public authorities; Freedom of Information (Designation as Public Authorities) Order 2015, designated, for certain of their functions, Network Rail Limited, Network Rail Infrastructure Limited and Network Rail Holdco Limited as public authorities.

⁶⁴ Freedom of Information (Scotland) Act 2002, s. 5(3).

⁶⁵ *Ibid.*, s. 5(2)(a).

⁶⁶ *Ibid.*, s. 5(2)(b).

⁶⁷ *Ibid.*, s. 5(1).

⁶⁸ *Ibid.*, s. 5(4).

⁶⁹ Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities) Order 2013 designated the following as Scottish public authorities: A body established or created solely by one or more local authorities, whose functions on behalf of any of those authorities include developing and/or delivering recreational, sporting, cultural or social facilities and activities, and which in carrying out those functions is financed wholly or in part by any of those authorities, when performing functions contained in ss 90 and 163 of the Local Governmental (Scotland) Act 1973, s. 14 of the Local Government and Planning (Scotland) Act 1982 or s. 20 of the Local Government in Scotland Act 2003; Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities)

Therefore, although certain institutions are identified as public authorities in the Schedule to the Acts, other bodies can be added by designation, in relation to functions of the body which appear to be exercises of a 'public function'. The list of public authorities therefore contains both *institutional and functional* approaches to defining public authorities. Private actors engaged in the performance of public functions can therefore be 'public authorities' for the purposes of the GDPR in the UK.

The definition of public authority in the freedom of information legislation also includes private bodies which are owned by public authorities. It is therefore considerably wide. A 'publicly-owned company' for the purposes of the 2000 Act is a company which is 'wholly owned' by the Crown,⁷⁰ the wider public sector,⁷¹ or both together.⁷² The wider public sector includes those authorities listed in Schedule 1 to the 2000 Act, save for those which are Government Departments or are 'listed only in relation to particular information'.⁷³ A 'publicly-owned company' for the purposes of the 2002 Act is a company which is wholly owned by the Scottish Ministers or a 2002 Act Schedule 1 public authority, save for those which are only listed in relation to 'information of a specified description'.⁷⁴

The Data Protection Bill, however, goes much further. Clause 7(2) states that 'an authority or body' defined by clause 7(1) is 'only a "public authority" or "public body" when performing a task carried out in the public interest or in the exercise of official authority vested in it'. This was an amendment to the Bill introduced at Report Stage.⁷⁵

The amendment has an important apparent effect. If an authority or body falls within clause 7(1) of the Data Protection Bill and is performing a task carried out in the public interest or in the exercise of official authority, it follows that the body is a public authority for the purposes of the GDPR and cannot rely on legitimate interests as a basis for processing. It can rely on Article 6(1)(e) GDPR. Therefore a 'private' actor can be treated as a public authority for the purposes of the GDPR when performing tasks in the public interest or exercising official power if appropriately designated.

However, when outside those public tasks and exercises of official authority, all public authorities defined by clause 7(1) also cease to be a public authority at all by virtue of clause 7(2). Therefore, public authorities can make use of legitimate interests as a basis for processing, irrespective of which interpretation of the limit on Article 6(1)(f) is preferred. This addresses 'hybrid' bodies with both public and private functions and clarifies that public authorities may rely on legitimate interest processing when performing tasks other than tasks in the public interest or in the exercise of official authority.

The UK Data Protection Bill therefore goes further than an *institutional and functional view* of Article 6(1) GDPR's application to 'public authorities in the exercise of its tasks'. A public

Order 2016, designated as a Scottish public authority grant-aided schools when performing the function of the running of a grant-aided school as defined in s. 135(1) of the Education (Scotland) Act 1980; independent special schools listed in the Register of Independent Schools as set out in s. 98 Education (Scotland) Act 1980 and fall within s. 29(1)(a) Education (Additional Support for Learning) (Scotland) Act 2004, when performing a function under s. 29 of the 2004 Act; Scottish Health Innovations Limited when promoting research and development within the NHS in Scotland; secure accommodation service providers as defined by Sch. 12(6) to the Public Services Reform (Scotland) Act 2010, when performing the function of the provision of a secure accommodation service; persons providing services under contract with, or a subcontract of that contract, the Scottish Ministers for the running of a prison or a part of a prison, when performing functions under s. 106(1) Criminal Justice and Public Order Act 1994.

⁷⁰ Freedom of Information Act 2000, s. 6(1)(a).

⁷¹ *Ibid.*, s. 6(1)(b).

⁷² *Ibid.*, s. 6(1)(c). See also *Ibid.*, ss 6(2) and 6(2A).

⁷³ *Ibid.*, s. 6(3).

⁷⁴ Freedom of Information (Scotland) Act 2002, s. 6.

⁷⁵ See Data Protection Bill (As amended on Committee), cl. 6. The clause was renumbered at Report Stage.

authority is only a public authority *at all* when processing data to which Article 6(1)(e) might apply. This is a *purely functional view*.

This collapses the public-private divide in relation to private actors engaged in the performance of tasks in the public interest, provided that they are suitably designated or publicly owned. This has a set of important corollaries. Such private actors, when performing Article 6(1)(e) tasks, must have a data protection officer, are protected from enforcement action outside the UK and could be exempted from administrative fines. However, traditional public authorities would seem to lose their protection from enforcement when not processing pursuant to Article 6(1)(e) GDPR.

This is positive as it allows many potential anomalies identified in relation to the public-private divide in the GDPR where private actors perform public functions to be removed. However, it relies on private actors performing public functions to be initially included within clause 7(1) and is also premised on the correctness of the institutional and functional view over the institutional view of Article 6(1) GDPR's restriction on legitimate interests processing. It goes beyond this in clause 7(2) by introducing a *purely functional view*. This may well be objectionable should the matter ultimately be considered by the CJEU, if it decided that the *institutional* view of Article 6(1) GDPR is correct. If that view is preferred, a *purely functional* view is both under and over inclusive: under inclusive, because it allows public authorities to rely on legitimate interests processing for *some* of their tasks, and over inclusive, because it unnecessarily prevents *some* private actors from relying on legitimate interest processing when performing public functions.

4. BLURRING THE PUBLIC-PRIVATE DIVIDE IN DATA PROTECTION

A well-constructed list of public authorities including all private actors involved in the exercise of public functions would be an effective solution to many of the concerns analysed above regarding the public-private divide in the GDPR. The anomalies are only mitigated however if private actors performing public tasks are in fact suitably designated or are in fact publicly owned and fall within the scope of clause 7(1).

However, there are also other problems and complexities to be overcome. First, the freedom of Information legislation seeks to enhance the transparency of public authorities. An important consideration for the definition of public authorities in this context is to prevent transparency of public functions being lost through contracting out or public ownership of private actors. In the context of the Human Rights Act 1998, Oliver noted that the approach proposed in freedom of information legislation might be regarded as a convenient model for the 1998 Act, which imposes duties on public authorities to comply with ECHR rights, but argued that this approach would be flawed because the 'concepts are used for different purposes' and 'the rationales for [freedom of information duties] are not the same as the implication of and rationales for imposing duties to respect Convention rights'.⁷⁶ The same point can be made of using freedom of information definitions for the purposes of the GDPR. It might not always be desirable that a private actor involved in the exercise of public functions should be defined as a public authority. Public authority in the context of the GDPR has implications for the lawful grounds of processing, obligations to appoint data controllers, and protections from certain types of enforcement. Whether a private actor with public functions should be included within the definition must reflect which set of obligations under the GDPR is most appropriate. To be effective therefore, the list must be very carefully tailored to ensure that the definition of bodies as public authorities does not unnecessarily undermine individual data protection rights or introduce arbitrary distinctions.

Secondly, in the context of human rights, Donnelly argues that private contractors should be subject to the 'same constraints as government' because the delegation of power through

⁷⁶ Dawn Oliver, *The Frontiers of the State: Public Authorities and Public Functions under the Human Rights Act*, PL 476, 480 (2000).

contracting out gives a private contractor 'enormous capacity to violate human rights'.⁷⁷ Contracting out otherwise has the potential to undermine human rights.⁷⁸ However, in the context of the GDPR and Article 8 CFR, classification as a public authority has mixed effects, restricting some rights and obligations and imposing other obligations. A broad definition of public authority is therefore not always an unqualified good for the individual in the case of the GDPR.

Thirdly, Oliver argues that we should be cautious to use an expansive definition of public authority because 'such treatment legitimises state control of a many activities by private bodies... thus rolling forward the frontiers of the state'.⁷⁹ In the context of the GDPR, to insist on a broad interpretation of public authorities will be to require many bodies to seek statutory authorisation for data processing activities, where legitimate interests were previously relied upon. The effect might be to expose those private bodies to centralised control and the vicissitudes of politics in obtaining a legal basis for processing. This has the potential to delay or stifle valuable innovation, a cost that should also be weighed against the benefits of an approach grounded in legality and enhancing transparency and democratic oversight.

Finally, the approach in the Data Protection Bill will only go some way to remove legal uncertainty, a problem faced by other definitions of public authority and public function, such as section 6 of the Human Rights Act 1998.⁸⁰ Section 6(3)(b) of the 1998 Act provides that the term 'public authority' includes 'any person certain of whose functions are functions of a public nature', but 'in relation to a particular act, a person is not a public authority by virtue only of subsection (3)(b) if the nature of the act is private.'⁸¹ Bamforth notes that this is 'intended to catch private (or ostensibly private) bodies which, as a result of processes of privatisation and contracting out, now perform public duties which were formerly the responsibility of government'.⁸² However, it has been subject to considerable debate and uncertainty in application. The Data Protection Bill carries a similar risk in clause 7(2) which requires a rational distinction to be drawn between functions which are 'performed in the public interest' or the 'exercise of official authority' and those that are not. This might be expected to produce similar problems to the distinctions between 'public functions' and 'private acts' in the Human Rights Act 1998.

Bamforth, writing on the Human Rights Act 1998, states that distinctions between public and private in law 'will depend... on one's underlying theories of justice and political morality'.⁸³ This is correct but it should not be neglected how far a detailed analysis of the rights and obligations at issue, and a practical and pragmatic assessment of the definitions effect on those rights, should shape our thinking about the best way to give concrete expression to Article 8 CFR and data protection in the GDPR and national data protection law.

A valuable analysis of the justification for a public-private divide in data protection can be found in the work of Blume. His analysis assumes a rigid distinction between public authorities and private actors consistent with an *institutional* view. A better public-private divide should focus more on a *functional* analysis, given the complexities of private actors involved in the exercise of public functions.

Blume and Svanberg acknowledge that 'the main argument in favour of uniform data protection rules for both the public and private sectors is that the level of protection should be

⁷⁷ Donnelly, *supra*. n.30 at 787.

⁷⁸ *Ibid.*, 787.

⁷⁹ Oliver, *supra*. n.76 at 492.

⁸⁰ See Donnelly, *supra*. n.30 at 790.

⁸¹ Human Rights Act 1998, section 6(5).

⁸² Nicholas Bamforth, *The application of the Human Rights Act 1998 to public authorities and private bodies*, CLJ 159, 159 (1999).

⁸³ *Ibid.*, 170.

the same in all parts of society and across the EU', especially as it is challenging to draw a 'clear and workable line between the two sectors'.⁸⁴

However, Blume also argues that a 'fundamental difference' between public and private controllers lies in the 'foundation' of data processing in statute or other law and contract respectively.⁸⁵ For Blume, it is important that individuals are subject to obligations to disclose information to public authorities,⁸⁶ whereas private data processing is voluntary.⁸⁷ The 'state has powers that private enterprises do not and also should not possess'.⁸⁸ Public authorities process data as the result of a 'fundamental democratic process' which sets their 'tasks and obligations'.⁸⁹ Blume considers that the more intensive regulation of public bodies through administrative law makes it arguable that those bodies could be subject to less regulation under data protection law.⁹⁰ State actions are 'most important for the well-being of citizens' and data processing is 'essential' for delivering its functions.⁹¹ Trust in data processing may also differ between public and private sectors,⁹² and is likely higher in the public sector, which is subject to this 'principle of legality'.⁹³ Therefore, Blume argues that 'data protection law could be less restrictive in the public sector'.⁹⁴ Different 'means should and can be applied in order to make the law efficient', reflecting 'special features of the two sectors',⁹⁵ so that specific rules and enforcement might differ between public and private bodies.⁹⁶ For example, Blume questions whether administrative fines are 'meaningful' to a public authority, where fines return to public funds.⁹⁷ He also comments that the right to erasure is 'most appropriate in the private sector'.⁹⁸ Public and private bodies also differ in their motivation for processing: public interest vs commercial interest.⁹⁹ Public and private bodies differ in their organizational structures.¹⁰⁰ Blume concludes that the case for specific data protection rules is stronger for private bodies, the opposite of the traditional human rights position.¹⁰¹

The difficulty of such an analysis is that it assumes a set of institutional differences that neatly demarcate public authorities from private actors. In fact, these are useful generalizations but are undermined in some circumstances, especially where private actors exercise public functions.

One can and should go further than Blume. Whether data processing should be based on statute, a data protection officer is required, and restrictions should be placed on enforcement outside the UK or via administrative fines should depend on whether the function is a public one. A *functional* analysis should drive the definition of a public authority and therefore which bundle of obligations attaches to it. Approaches in freedom of information, human rights and

⁸⁴ Peter Blume and Christian Wiese Svanberg, *The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Public/Private Sector Divide and the Bureaucratic Apparatus*, p. 30.

⁸⁵ Blume, *supra*. n.9 at 299.

⁸⁶ Blume, *supra*. n.7 at 34; Peter Blume, *Impact of the EU General Data Protection Regulation on the Public Sector*, 1(1) *Journal of Data Protection and Privacy* 53, 54 (2016).

⁸⁷ Peter Blume, *The Inherent Contractions in Data Protection Law*, 2(1) *International Data Privacy Law* 26, 32 (2012); *Ibid.* (2016), 54.

⁸⁸ Blume, *supra*. n.7 at 34.

⁸⁹ Blume and Svanberg, *supra*. n.84 at 31.

⁹⁰ Blume, *supra*. n.7 at 34.

⁹¹ *Ibid.*

⁹² *Ibid.*

⁹³ *Ibid.*

⁹⁴ *Ibid.*

⁹⁵ *Ibid.*, 35.

⁹⁶ *Ibid.*

⁹⁷ Blume, *supra*. n.86 at 60.

⁹⁸ Blume, *supra*. n.87 at 33; Blume, *supra*. n.86 at 57.

⁹⁹ Blume, *supra*. n.9 at 299.

¹⁰⁰ *Ibid.*, 300.

¹⁰¹ *Ibid.*; see also Blume and Svanberg, *supra*. n.84 at 31.

other legal regimes cannot be straightforwardly borrowed. The need for democratic control and legitimacy through statutory processing, the need for data protection officers, and the appropriateness of exposure to enforcement in other Member States or administrative fines do not necessarily lend themselves to a rigid demarcation of public and private actors on an *institutional* basis. Rather, a more nuanced *functional* analysis is required, especially in the case of private parties exercising public tasks.

5. CONCLUSION: THE FUTURE OF THE PUBLIC-PRIVATE DIVIDE IN THE UK

The UK Government's decision to trigger Article 50 and initiate Brexit is a political event of enormous significance. European influence will not cease, although its processes and pressures will alter, after Brexit. It seems likely that the UK will maintain essential equivalence with the GDPR to secure an adequacy decision for the purpose of cross-border data flows.

The UK approach could be developed to enable a highly tailored definition of public authorities, which is capable of addressing many of the problems identified with the public-private divide in data protection, especially where private actors exercise public functions. This is a challenging undertaking and it is necessary to avoid arbitrary distinctions. The UK should seek to categorize bodies with care to promote certainty and unduly restrict neither appropriate innovation via legitimate interests processing nor the rights of data subjects where private bodies are involved in the performance of public functions. This should be achieved by focusing on a *functional* approach to the definition of public authorities and ensuring a broad coverage of private actors performing public functions through clause 7 of the Data Protection Bill.