Has the 2016 General Data Protection Regulation really given consumers more control over their personal data?

Bethany Sealey, Liverpool John Moores University

Abstract:

The General Data Protection Regulation (GDPR) - in force from May 2018 - introduced significant changes to data privacy laws. It appears to put data subjects in charge, with new and improved subject rights, wider territorial scope, and increased accountability and enforcement mechanisms, all of which aims to strengthen individual rights. This 'digital revolution' presented the existing data protection legislation, namely the Data Protection Directive (DPD) (1995), with significant challenges, however. New means of processing personal information have led to increased consumer concerns over just how personal data is gathered, handled, and stored. Modern - and largely intangible - processing methods may result in data subjects lacking control over their personal data: control is an essential aspect of data protection, not only in terms of privacy, but to uphold informational autonomy. As their own data is affected, a consumer should be able to '…predict with sufficient certainty which information about himself in certain areas is known to his social milieu…' Having the right to choose how data is dealt with and where it will eventually end up is key. This article analyses what the new Regulation has achieved but also questions the way in which it has affected consumers.

1. Introduction

The General Data Protection Regulation (GDPR)[1] - which came into force in May 2018 - introduced a complete change to data privacy law. Arguably one of the most comprehensive pieces of European Union legislation,[2] the GDPR appears to put data subjects in charge, with new and improved subject rights, wider territorial scope and increased accountability and enforcement mechanisms, all of which aim to strengthen their individual rights. The digital revolution presented the existing data protection legislation, namely the Data Protection Directive (DPD) (1995),[3] with significant challenges. New means of processing personal information have led to increasingly acute consumer concerns over how personal data is

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC [2016] OJ L 119/1 (Henceforth GDPR)

[2] M Kedzior, "GDPR and Beyond – A Year of Changes in the Data Protection Landscape of the European Union." *ERA Forum* (2019) 505

[3] 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 [1995] OJ L 281/31 (Henceforth DPD)

gathered, handled, and stored. Modern - and largely intangible - processing methods may result in data subjects lacking control over their personal data. Control is in itself an essential aspect of data protection, not only in terms of privacy, but to uphold informational autonomy.[4] As their own data is affected, a consumer should be able to '…predict with sufficient certainty which information about himself in certain areas is known to his social milieu…'[5] in order to have control over it. This may be done by having the right to choose how data is dealt with and where it will eventually end up.

This article analyses what the Regulation has achieved in relation to giving consumers more control over their personal data. The wording and principles of the GDPR appear to prioritise consumer control, more so than any other European legal instrument. The issue of how GDPR has affected consumers has however received far less attention than the repercussions of the legislation upon organisations. Much academic commentary has focused upon commending, comparing or criticising the European initiative: this article will look to these to gauge whether this 'gold standard' reform really 'does what it says on the tin.' It compares GDPR with DPD to set out the rationale for reform, having regard to the increased influence and advance of modern technologies in a globalised market; it then argues that the breakdown of technological boundaries means that the DPD had perhaps lost touch, in terms of territorial scope, definitions, and terminologies. It therefore then examines those rights and principles that give rise to greater consumer control over personal data, not least transparency, fairness, lawfulness, and accountability.

Arguably, such changes were not truly ground-breaking, given that these principles are similar to those set out in the earlier Directive. The rights contained in the 2016 Regulation clearly reinforce these core principles however, not least the rights to be forgotten, to have data access, and portability. An enforcement mechanism is a crucial aspect of consumer control. The conclusion argues that, despite clearly improving individual control, the Regulation may still not provide adequate protection when it comes to the most advanced areas in the technological field, namely, where mechanisms automatically or unknowingly process personal data. With this area of law constantly developing, however, it may be premature to critique certain obscure methods of processing: UK citizens similarly face a perhaps unknowable future post-Brexit. The concept of data protection remains a fundamental right however, given how the Charter of Fundamental Rights of the European Union works alongside the GDPR to uphold individual rights. In other words, both the Regulation – and the concept of a right to data protection - may be redundant if existing in isolation; they must rely upon each other to operate effectively.

[4] M Tzanou, "Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not so New Right" *International Data Privacy Law* (2013) 88-99

[5] S Gutwirth, Y Poullet, P de Hart, C de Terwangne and S Nouwt, *Reinventing Data Protection?* (Springer, 2009) 53

2. Let's talk about data protection…

The frenzy following the enactment of the General Data Protection Regulation (EU) (2016/679) reflects the significance and far-reaching implications of the changes to this legal framework. One of the most progressive pieces of EU legislation, the GDPR completely restructures how data is gathered, handled, and stored. Repealing the previous Data Protection Directive 95/46/EC, the Regulation laid out rules for businesses and natural persons alike, on the free movement of personal data within the European Union (EU). As well as providing a higher level of protection for personal data, a primary objectives of the GDPR was to increase consumer control, as stated in the first article. The objectives of data protection and privacy law have transformed from preventing fraudulent usage of data to placing EU citizens in the driver's seat. New protections, included the right to erasure, data portability, and the right to rectify inaccurate data, so that consumers are now closely involved in personal data management. The increasing influence of computers since the 1970's has seen personal data become digitalised and much more accessible to organisations.[6] Numerous data protection measures have been enacted, to address the exponential growth of technology. The UK's Data Protection Act (1984) was the first to provide a legislative framework for how 'automatically processed information' is dealt with. It required those processing the data ('data users') of "living individuals who can be identified by that data" [7] to register with the Data Protection Registrar. Sanctions for breaches – including criminal prosecution[7] - and compensation for individuals affected by inaccuracy,[8] loss[9] or unauthorised destruction[10] of data, were also introduced. Subsequent European initiatives (Data Protection Directive 95/46/EC) sought to regulate free movement of personal data across Member States. Similar to the 1984 Act, this Directive outlined guidelines for processing personal data, the rights of data subjects, and also updated definitions of key terminology.

Over time, this once innovative Directive began to stagnate, unable to keep up with the fresh challenges of an increasingly digital age. Viviane Reding, vice-president of the European Commission (from 2010-2014), stressed the need for a "comprehensive and coherent approach" to data protection legislation.[11] One of the primary challenges identified was the ruthless advance of modern technologies: social media, mobile phones connected to the internet and greater availability of Wi-Fi enabled data to be transferred quickly and easily. This led to many consumers failing to exercise caution in respect of, for example, the type of data they share, and the motives of its potential recipients. These new platforms have also enabled businesses and other organisations to buy and sell consumers' personal data for the purposes of marketing, advertising, or fundraising. When the DPA was implemented in 1998, a mere 9%

[6] P Carey, *Data Protection* (2018) (5th Edn. Oxford University Press) 2
[7] Data Protection Act [1984] s.19(2)
[8] Ibid s.22(1)
[9] Ibid s.23(a)
[10] Ibid s.23(b)
[11] V Reding, "The Upcoming Data Protection Reform for the European Union" *International Data Privacy Law* (Vol.1, 2011) 3

of UK households had access to the internet.[12] This increased to 77% at the time of Reding's analysis in 2011, and further soared to 90% by 2017.[13] The 'algorithmic' decision-making incorporated into technological advancement, has made it difficult for individuals to control, or to at least feel in control, of their personal information.[14] Technology is now capable of making predictions and decisions automatically; [15] with little to no human involvement in how or when data is processed, it is particularly difficult to prevent it being dealt with via these services. (The issues with automated decision-making systems, particularly blockchain technology, will be discussed further below).

An additional challenge was globalisation.[16] By blurring the contours of data movement, globalisation has seen data transferred to jurisdictions outside of the EU and beyond the Directive's authority. Reding identified the need for secure data management by law enforcement authorities, in exceptional circumstances.[17] Modern technology has however allowed for data-sharing for 'surveillance purposes,' for example where suspected terrorist activities might threaten public security.[18] Chapman notes further that the 'Internet of Things,' (IoT) - any device that can store data through internet access - has revolutionised how authorities gather evidence, e.g. via data on smart watches or car systems.[19] Although using data in this way may fall within public interest, it still must ensure that rights are not being breached. Such challenges permit scepticism regarding the effectiveness of the Directive; Reding maintains the importance of the core principles outlined in the DPD however. [20] The Directive operated effectively in its day, but failed to adapt, justifying a significant overhaul. GDPR builds upon the pre-existing framework, but attempts to address persistent challenges, so that consumers in the digital age gain greater awareness of - and control over - their sensitive data.

3. Battle of the EU Statutes

When assessing whether the GDPR awards its subjects with higher levels of control over their personal data, it is useful to compare current legislation with its predecessor. The Regulation was produced in response to the fresh challenges of the digital age: complete restructure of the legislative regime - from Directive to Regulation – followed, with implications for the scope and application of both mechanisms. New rights and obligations were introduced by the GDPR, refining definitions and key terminologies, all of which allows for analysis of the extent to

[12] Office for National Statistics, "*Internet Access- Households and Individuals*" (ONS, 1998)
[13] Office for National Statistics, "*Internet Access- Households and Individuals*" (ONS, 2017)
[14] J E Cohen, "Turning Privacy Inside Out" *Theoretical Inquiries in Law* (Vol 20, 2019) 2
[15] C Castelluccia and D Le Metayer - European Parliamentary Research Service. "Understanding Algorithmic Decision- Makin: Opportunities and Challenges." *Panel for the Future of Science Technology* (2019)3
[16] Reding (n 11) 3
[17] Ibid
[18] M Zalnieriute, "Developing a European Standard for International Data Transfers after Snowden: Opinion/15 on the EU-Canada PNR Agreement" *Modern Law Review* (Vol 81, 2018) 1054

which consumers now might have more control over their data. Article 288 of the Treaty of the Functioning of the European Union (TFEU) [2009] states that a Regulation shall be "binding in its entirety and directly applicable in all Member States."[19] Directives have a similarly binding character but allow for Member States to enact the Directive separately into domestic law. As a Regulation, the GDPR surpasses the authority of the previous DPD. Instead of Member States interpreting the Directive - and incorporating it into their own personal data protection laws - the new regime applies uniformly across the EU. Presumably, this was an intentional strategy to ensure harmonious and consistent application [20] and speedy enactment.[21] Prior to GDPR, contrasting data protection laws across multiple nations caused much conflict, especially where a data subjects were located in a different state to that of the controller.[22]

Weltimmo explored whether enforcement action could be taken by the Hungarian data protection authority against a company in Slovakia. The Court of Justice of the European Union (CJEU) decided that the authority seeking to exercise their own national laws (Hungarian law) were able to do so, but that its enforcement powers were 'limited to its territory.'[23] Thus, the Hungarian authorities could use their investigative powers under their own procedural law, but did not have jurisdiction to enforce fines upon the Slovakian company. It could be argued that, due to the nature of data protection, the only way in which to address this issue is to adopt a homogenous set of rules. And yet, due to globalisation, it would be impossible to allow adaptations of the statute across borders that have become blurred through our 'interconnected age.' As Politou et al note, due to conflicting national cultures and priorities, some of the provisions under the GDPR will likely still leave scope for differing interpretations.[24] Territorial scope is outlined in Article 3: it concerns data processing within the EU, but also data transactions between European Union (EU) subjects and organisations operating outside of its jurisdiction. Non-Member States must comply with the EU law as well as their domestic legislation.[25] Previously, Article 4(1)(a) outlined the territorial range of the DPD, where:

> …the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

[19] Treaty of the Functioning of the European Union (TFEU) [2009] Art. 288
[20] M Kedzior (n 2) 507
[21] Ibid
[22] J Hörnle, "Juggling more than three balls at once: multilevel jurisdictional challenges in EU Data Protection Regulation" *International Journal of Law & Information Technology* (Vol 27, 2019) 147
[23] *Weltimmo s.r.o.v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] C-230/14
[24] E Politou, E Alepis and C Patsakis, "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions" *Journal of Cyber Security* (2018)4
[25] C Tikkinen-Piri, A Rohunen, J Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Compute Law and Security Review* (Vol 34, 2018) 135

Compared to the GDPR, the Directive only applied to processing occurring within the territory of each Member State. The CJEU widened this scope in *Google Spain SL & Google Inc. v Mario Costeja Gonzalez* [2014] to include subsidiaries processing personal data within the EU on behalf of their foreign parent company.[26] Although *Google Inc*. was considered a US organisation, the CJEU ruled that the activities of the subsidiary in Spain constituted sufficient "establishment" and were therefore required to comply with the new Directive.[27] The CJEU further considered territorial scope in *Weltimmo* [2015], where establishment was deemed to be present if the controller carried out "real and effective activity – even a minimal one" within the Member State.[28] The term "establishment" applies to any subsidiaries offering goods and services within the EU, but also encompasses all processors or controllers processing personal data, including the monitoring of behaviour, of EU citizens, regardless of membership status. Such increased territorial scope provides a higher level of protection for data subjects, but the provision is still prone to ambiguities.

The activity of extraterritorial organisations, including the United Kingdom post-Brexit, may be difficult to regulate (and is discussed below).[29] Hörnle further highlights the lack of clarity surrounding territorial application of the Regulation. Neither the DPD nor the GDPR specifies whether processing applies solely to EU residents or extends to individuals whose data is processed while they are temporarily present within the EU.[30] This 'grey area' may restrict territorial scope, or result in wrongful enforcement and "extraterritorial overreach."[31] GDPR seems likely to be applicable where there is reasonable connection between the subject and the EU - such as residency - but once again it may be difficult to distinguish the data of EU citizens from that of non-residents.

4. Key terminologies

Definitions under the DPD were not synonymous across all Member States: this led to uncertainty over the implementation of core principles.[32] One of the most significant developments was the changing definition of 'personal data.' This previously included:

> "…any information relating to an identified or identifiable natural person… who can be identified, directly or indirectly, in particular by reference to an

[26] *Google Spain SL & Google Inc. v Mario Costeja Gonzalez* [2014]C-131/12
[27] O Lynskey, "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez" *Modern Law Review* (2015) 225
[28] *Weltimmo s.r.o.v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] C-230/14
[29] Carey (n 6) 7
[30] Hörnle, (n 22) 161
[31] Ibid
[32] Carey (n 6) 8

> identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[33]

Auld LJ took a narrow approach in *Durant v Financial Services Authority* [2003] stating that a "mere mention of the data subject in a document held by a data controller does not necessarily amount to his personal data."[34] Here, 'personal data' must either be 'biographical' or the affected individual must be the specific focus of the data. The European Commission felt that this case demonstrated misapplication of the Directive.[35] Durant emphasized the ambiguity within the Directive's definitions, particularly the UK's Data Protection Act's need for a "…better framework for striking the appropriate balance between personal data and subject access rights."[38] Rempell highlights discrepancies, including the unnecessarily narrow interpretation of 'relating to' and the wrongful use of data subject access provisions (outlined in the implemented UK law) [36] which allowed courts to narrow the definition further via the notion of 'focus.'[37] A wider approach is seen in *Edem v IC & Financial Services Authority* [2014] which held that "a name is personal data unless it is so common that without further information, such as its use in a work context, a person would remain unidentifiable despite its disclosure."[38] This included not only names, but also email addresses, phone numbers, home addresses and ID numbers, anything that can identify a natural person.[39] Since the Directive, personal information can be accessed through a plethora of platforms: GDPR attempted to address this ambiguity by expanding the definition to:

> "Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[40]

'Personal data' now includes anything that can be used to identify individuals.[41] According to the Information Commissioner's Office (ICO) this includes ID numbers, addresses and other

---

[33] Data Protection Directive 95/46/EC section 2(a)

[34] *Durant v Financial Services Authority* [2003] EWCA Civ 1746

[35] S Rempell, "Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: *Durant v Financial Services Authority* as a Paradigm of Data Protection Nuances and Emerging Dilemmas" *Florida Journal of International Law* (Vol. 18, 2006) 823 at 841

[36] The Data Protection Act 1998

[37] Rempell (n 35) 823-827

[38] *Edem v IC & Financial Services Authority* [2014] EWCA Civ 92

[39] See Unity "*The Main Differences Between the DPD and the GDPR and How to Address Those Moving Forward*" (British Legal Technology Forum, 2017)

[40] GDPR Art. 4(1)

[41] Politou et al (n 24) 3

locational data, and such 'online identifiers' as IP addresses and cookie IDs,[42] many of which were unheard of at the time of the DPD. This contradicts Durant, confirming that individuals can be identified solely by name, deeming it 'personal data.' Carey argues that the term 'natural person' only relates to living individuals: rights cease upon death.[43] Although the provision only protects individuals, information collected in a company environment may be covered. The Regulation fails to distinguish between data processed at work or in one's personal life.[44] A wider interpretation of 'personal data' is key to increasing consumer power, as it applies to an almost unlimited quantity of data, provided that data relates to the affected individual in some way. It may however be difficult for consumers to exercise control over data that is spread across multiple platforms. Clearly, domestic courts must continue to apply the broader meaning of personal data, prevent further inconsistencies, as in Durant.

Some definitions have remained consistent across the DPD and the GDPR (such as 'processing,'[45] 'controller'[46] and 'processor,'[47]) although the Regulation has introduced new terminology. 'Profiling' is a type of automated processing that uses personal data to predict "personal aspects relating to a natural person" such as interests, behaviour, location or movements etc.[48] With rapid technological development, data 'profiles' have become more comprehensive, allowing more opportunity to identify individuals through profiled, sensitive information. [49] Such profiling enable companies to advertise personalised services to consumers. Originally dubbed 'market manipulation,' as Calo notes, profiling could promote certain products to unsuspecting, vulnerable consumers. Within the Internet of Things, this has paved the way for specialist exploitation of the masses.[50] Although profiling is perfectly legal - and widely used as a method of collecting data - it may lead consumers to feel out of control; intangible, sometimes unascertainable, are created by companies without their understanding. As Eskens argues, the Regulation must encourage transparency over profiling. [51] Under Article 29 of the Working Party Opinion on the Internet of Things, greater transparency may require companies to identify reasons behind profiling, so that consumers can make informed decisions on whether to consent to such data usage.[52] 'Pseudonymisation' is a further type of data, processed in such a way that it can no longer be related back to the data subject without an unlocking 'key.'[53] Such processing provides an extra layer of protection for data subjects – and

[42] ICO https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-dataprotection-regulation-gdpr/key-definitions/what-is-personal-data/ (accessed 30.06.20)
[43] Carey (n 6)14
[44] Ibid
[45] GDPR Article 4(2)
[46] GDPR Art. 4(7)
[47] GDPR Art. 4(8)
[48] GDPR Art. 4(4)
[49] S Eskens, "Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should it?" *Institute for Information Law* (2016) 1
[50] R Calo, "Digital Market Manipulation" *The George Washington Law Review* (Vol 4. 2014)
[51] Eskens (n 49)
[52] Opinion 8/2014 on Recent Developments on the Internet of Things, (WP 223), 16 September 2014.
[53] GDPR Art. 4 (5)

controllers - who may need access to necessary data without requiring specific details about the consumer.[54]

It is essential to define what is meant by consumer control however: Westin's definition of 'privacy' drew upon individual control over the information that they choose to communicate to others.[55] Westin observed that a 'desire for privacy' was often against a 'desire for disclosure and communication of himself to others.'[58] The pivotal focus here is the notion of individual power to reveal only what is desired. This assumes that consumers have sufficient knowledge and understanding of the platforms they are using to enable them to control and safeguard their personal data. Arguably, the GDPR provides such control through the 'right to be forgotten' (discussed below). Its wider scope may mean that the GDPR stays relevant for longer, kept updated within a continually growing age of information.

5. GDPR Rights, Obligations and Principles that Enhance Control: Data Protection Principles of Lawfulness, Fairness and Transparent Data Processing

Several core principles underpin the GDPR: data minimisation,[56] accuracy,[57] storage limitation,[58] integrity, confidentiality and security,[59] all of which contribute to enhanced consumer control. Expanding upon the original data protection principles set out in the earlier Directive, Article 5 (1)(a) [GDPR] dictates that "personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject." Data processing will only be considered lawful where it complies with one of Article 6's conditions, all of which – excluding Art. 6(1)(a) – require processing to be carried out only for a 'necessary' purpose.[60] Case law defines that which is 'necessary.' In *Gillow v United Kingdom* [1986], 'necessity' indicated a 'pressing social need.'[61] *Huber v Germany* [2009] stressed that any measure carried out by the state should be '…proportionate to the legitimate aim pursued.'[62] Carey emphasised the distinction between merely 'useful' or 'convenient' processing and processing that is 'necessary.'[63] Processing cannot be lawful unless there is pressing and justifiable requirement.

The primary lawful condition concerns the provision of consent by the data subject, allowing the controller to use their personal data "…for one or more specific purposes."[64] The GDPR defines consent as:

[54] Carey (n 6) 96
[55] A Westin, *Privacy and Freedom* (Ig Publishing New York, 1967)
[56] GDPR Art. 5 (1)(C)
[57] GDPR Art. 5 (1)(D)
[58] GDPR Art. 5 (1)(E)
[59] GDPR Art. 5 (1)(F)
[60] GDPR Art. 6(1)(f)
[61] *Gillow v United Kingdom* [1986] ECHR 9063/80
[62] *Huber v Germany* [2009] CMLR 49
[63] Carey (n 6) 50
[64] GDPR Art 1(a)

> "…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[65]

According to the ICO, 'freely given' means that the consumer has an honest and informed choice to either agree or refuse the processing of their personal data. [66] This includes an option to reject or revoke consent already given; refusal of consent must be 'without detriment,' and consent given under duress is invalid. Should a company deny access to their website - on the basis that a consumer has either refused or revoked consent to the company's personal data processing terms and cookie policies – it would breach Article 4. Companies must allow data subjects to access goods and services, regardless of whether or not they have consented to the processing of their personal information. ICO asserts that 'informed' consent requires companies to actively make consumers aware of what they agree to - or disagree with – via clear language that is 'separate from other terms and conditions.' [67] Any misleading of consumers via confusing language automatically invalidates consent. Preventing companies from misleading consumers reinforces the 'fair' and 'transparent' aspects of data protection principles. Consent at this stage engenders consumer control, given their power to consent to or reject any data processing request. [68] The importance of consent during every stage of data processing can be seen through the Court of Appeal's judgement in *Richard Lloyd v Google LLC* [2019], where Google tracked cookies with neither the knowledge nor consent of the claimant. The case recognised how data processing without consent is a 'loss of control of personal data.' [69] However, this decision may yet open the floodgates as, "compensation could be claimed for any breach of data protection legislation regardless of its triviality or inconsequentiality." [70]

Data processed 'transparently' will make data subjects aware of how their data will be handled. Data controllers must frame data processing terms and conditions in comprehensive, unambiguous language that will not mislead the consumer.[71] The need for transparency is of greater importance in the IoT as data processing is largely intangible and secretive: consumers may not fully understand where their data goes unless explicitly told. [72] Transparency is a longstanding principle of EU (and UK) legislation and policy making, key to maintaining

---

[65] GDPR Article 4 (11)

[66] The Information Commissioner's Office, "Guide to the General Date Protection Regulation (GDPR)" (ICO, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/lawfulness-fairness-and-transparency/>, pp.20-23

[67] Ibid

[68] I Van Ooijen and H Vrabec, "GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective." *Journal of Consumer Policy* (2019) 94

[69] *Richard Lloyd v Google LLC* [2019] EWCA Civ 1599

[70] A Wills, "*Richard Lloyd v Google LLC* – Landmark Judgement in Representative Data Protection Action." *Entertainment Law Review* (2020) 56

[71] Carey (n 6) 44

[72] The Information Commissioner's Office, "Guide to the General Date Protection Regulation (GDPR)" (ICO, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/lawfulness-fairness-and-transparency/>, pp.20-23

confidence in the legislative process. It ensures that GDPR is adhered to by controllers and legislative bodies alike. In their guidance, the Article 29 Working Party state that transparency, "empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights."[73] Accountability has substantial weight too:[74] requiring data controllers to take appropriate measures to ensure compliance, upholds subject rights and maintains transparency.[75] Article 83 lays out the fines available should a company fail to meet the conditions of the Regulation, if records are outdated or inadequate. Accountability is thus vital in "…building consumer trust"[76] and "giving people the tools to exercise control."[77] Because the burden of accountability rests with the controller, consumers should have more trust in companies to not misuse their data. The complexities of data processing demand that accountable processing be both fair and 'sustainable.'[78] And yet, in practice, implementation may be onerous. As Kuner et al note,

> "…it may not be feasible for a human to conduct a meaningful review of a process that may have involved third-party data and algorithms (which may contain trade secrets), pre- learned models, or inherently opaque machine learning techniques."[79]

Although it may be difficult to understand where personal data goes once consent is given, if the data controller presents processing terms and conditions in a comprehensive, descriptive way, using plain language, it will adhere to the Regulation: the company has demonstrated sufficient accountability as the data subject has been presented with sufficient information to provide valid consent.

[73] Article 29 Working Party, "Guidelines on Transparency under Regulation 2016/679" (European Commission,

[74] S Bhaimia, "The General Data Protection Regulation: The Next Generation of EU Data Protection" *Legal Information Management* (2018) 21-26

[75] The Information Commissioner's Office, "Guide to the General Date Protection Regulation (GDPR)" (ICO, 2019)<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/accountability-principle/>

[76] A Crabtree, T Lodge, J Colley, C Greenhalgh, K Glover, H Haddadi, Y Amar, R Mortier, Q Li, J Moore, L Wang, P Yadav, J Zhao, A Brown, L Urquhart, D McAuley, "Building Accountability into the Internet of Things: the IoT Databox Model" *Journal of Reliable Intelligent Environments* (2018) 39

[77] Ibid 42

[78] G Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard" *International Data Privacy Law* (Vol. 6, 2016)

[79] C Kuner, D Jerker, B Svantesson, F H. Cate, O Lynskey and C Millard, "Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?" *International Data Privacy Law* (Vol. 7, 2017) 1-2

6. **Rights and obligations introduced under GDPR that award control to consumers**

New or revised rights and obligations for data subjects and controllers promote greater control and strengthen core principles. 'Subject access rights' (of data access) enable consumers to request status and whereabouts of their data at any point during its processing.[80] Individuals can make a 'data subject access request' (DSAR). Compared to its successor, the time constraint for a DSAR under the DPD was "…without excessive delay or expense."[81] The GDPR has narrowed this to "…one month of receipt of the request."[82] For data subjects, a tighter deadline means less uncertainty and more power, should the time limit be breached. However, this time restriction may place considerable pressure upon businesses, especially where multiple requests occur simultaneously.[83] To combat this, the GDPR permits companies to extend the deadline by up to two months where necessary.[84] The right to data portability also entitles consumers to request their data via transfer between controllers.[85] Recital 68 states that data portability is intended "to further strengthen the control of…data."[86] The purpose of data portability is to 'empower' individuals to freely and easily relocate their data, provided other party is willing and able to accept the said data and transfer it into their own systems. Companies can advertise their compatibility with Article 20, "...improving competition on the market," and giving them the edge over other organisations.[87] Arguably, this awards no control: it relies upon acceptance of the alternative service. It may be challenging also to align two completely different data systems. As Van Ooijen and Vrabec note, data portability means visualising' data in an apparently invisible system of personal data processing: they lambast Article 20 for its lack of clarity however, on the status of the data remaining in the previous service:"… It does not automatically mean that the data is removed from the original location and deleted."[88] Graef et al reject data portability in rights terms: they maintain that portability ought to "…be seen as a new regulatory tool in EU law that aims to stimulate competition and innovation in data- driven markets."[89] As a result, it would seem that this 'right' only confers incomplete control to consumers.

[80] GDPR Art. 15 (1)
[81] DPD Art 12 (a)
[82] GDPR Art. 12 (3)
[83] ITGP Privacy Team, *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2nd Edn. IT Governance Publishing, 2017) 192
[84] The Information Commissioner's Office, "Guide to the General Date Protection Regulation (GDPR)" (ICO, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/lawfulness-fairness-and-transparency/> from p.50
[85] GDPR Art. 20
[86] Recital 68, Regulation 2016/679 etc.
[87] R Janal, "Data Portability – A Tale of Two Concepts" *Journal of Intellectual Property* (2017) 60
[88] Van Ooijen and Vrabec (n 68) 103
[89] I Graef, M Husovec and N Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" *German Law Journal* (2018)1359

The right to erasure, otherwise known as 'the right to be forgotten' (RTBF), is a further consumer control right.[90] In certain circumstances, subjects can have their personal data deleted from the controller's database,[91] for example, if processing of personal data no longer aligns with its original purpose. [92] The RTBF places the onus upon companies to notify other organisations about erasure, where personal data has either been disclosed to others or made public in an online environment.[93] Although the individual would have to satisfy Article 17 conditions, it should be easy to invoke the RTBF. Allowing consumers to dictate when their data can be withdrawn and/or no longer processed, grants them significant control. Prior to the new Regulation, once data was released into an online processing system (where it could be reproduced exponentially) it would have been near-impossible to track, let alone erase.[94] Consumers undeniably have more control now over the 'scope' and 'flow' of their data. [95] And yet, the RTBF has seen considerable criticism, in terms of potentially undermining freedom of expression, where permitted material might perhaps be removed needlessly alongside personal data.[96](Arguably, penalties for non-compliance could perhaps be reduced.[97])

Exceptions to the RTBF under Article 17 (3) include scenarios where processing is necessary for: freedom of expression, compliance with legal obligations, public interest (i.e. health, historic or scientific research) or legal claims.[98] Consumer interests must outweigh those of the controller, for erasure to continue; determining balance may be problematic, with the Regulation failing to clarify when consumer rights must override other fundamental rights. Minor processing is unlikely to affect the privacy of the consumer; that which is excessive (placing privacy rights at risk) demands remedy. [99] The legislation seems to contradict this, as processing applies to all personal data, regardless of whether or not it is 'unlikely' to engage privacy rights. It may be unrealistic to try and retrieve all personal content from an indefinite list of controllers. Politou et al further highlight the practical difficulties. Once consent is passed to the controller, they have authority to do with it as they please; locating all controllers, including third parties (subjects and controllers may have no knowledge of some of them) could be an impossible task.[100] GDPR clearly falls short on defining when the RTBF should be enforced on a third-party basis.

---

[90] Van Ooijen and Vrabec (n 68) 102

[91] GDPR Art. 17

[92] GDPR Art 17 (a)

[93] The Information Commissioner's Office, "Guide to the General Date Protection Regulation (GDPR)" (ICO, 2019) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/principles/lawfulness-fairness-and-transparency/>, p.120

[94] Van Ooijen and Vrabec (n 68) 103

[95] Ibid

[96] E Adams Shoor, "Narrowing the Right to be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation." *Brooklyn Journal of International Law* (2014) 487

[97] Ibid, 518

[98] GDPR Art. 17 (3) (a-e)

[99] M Dunphy-Moriel and A Dittel," Forget me Not: Limits to the Right of Erasure" *Computer and Telecommunications Law Review* (2020) 22

[100] Politou et al (n 24) 11

A further 'right' has arguably emanated more from academic literature and discourse rather than from the explicit language of the Regulation. The 'right to explanation' concerns subject information collected through automatic processing, either by algorithms or artificial intelligence.[101] Such 'algorithmic accountability' enables consumers to request explanation about personal data processed automatically.[102] This may be a purely academic construction,[103] but it is relevant when determining whether consumers have any control over the more ambiguous aspects of internet processing. They must have understanding of the way in which their data gets processed in order to have control over it, which is a bewildering notion where intangible, automated processing is concerned.[104] As Selbst and Powles argue, the 'plain text of the GDPR' clearly provides a right to explanation:[105] the right to 'meaningful information about the logic involved' in automated decision making[106] (as seen in Articles 13-15) must also give rise to it in some form. A functional and flexible interpretation is key. A functional interpretation upholds transparency and subject autonomy, by providing an explanation of automated processing that is sufficient for informed decision-making on whether or not to consent.[107] This is particularly so when algorithmic formulae are complex. It is important to prevent an "unnecessarily constraining [of] research and development," which might occur should via rigid interpretations.[108] This positive analysis aims to focus on what the provisions can achieve rather than on what they might restrict.

Wachter et al doubt any existence of a right to explanation under Article 22(3) safeguards however, and stress instead the restrictions of Article 22(1): "The data subject shall have the right not to be subject to a decision based solely on automated processing…"[109] The use of the term 'solely' means that any human alteration or involvement in 'automated processing' means that it no longer is automated, rendering it irrelevant, and the right non-existent.[110] Selbst and Powles argue that such narrow interpretations fail to consider those other provisions within the GDPR that clearly support the right to explanation.[111] Mendoza and Bygrave argue that a right to contest automated decisions would be pointless if one did not know what the decision actually was, thereby creating a right to explanation.[112] The debate continues on whether

[101] S Wachter, B Mittelstadt and L Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* (Vol 7. 2017) 77
[102] M E Kaminski, "Right to Explanation, Explained" *Berkeley Technology Law Journal* (2019)
[103] B Goodman and S Flaxman, "European Union Regulations on Algorithmic Decision-Making and a 'Right to Explanation'" *AI Magazine* (2017) 50
[104] Van Ooijen and Vrabec (n 68) 97
[105] A D Selbst and J Powles, "Meaningful Information and the Right to Explanation." *International Data Privacy Law* (Vol 4, 2017) 235
[106] GDPR Art. 13 (F)
[107] D Selbst and J Powles (n 105) 236
[108] Ibid
[109] GDPR Art. 22(1)
[110] Wachter et al (n 101) 92
[111] D Selbst and J Powles (n 105) 234
[112] I Mendoza and Lee A Bygrave, "The Right Not to Be Subject to Automated Decisions Based on Profiling" *University of Oslo Faculty of Law Legal Studies Research Paper Series No.2017-20* in T Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer, Cham, CH 2017) 16

consumers should have understanding and control over content handled automatically: the right to explanation is however clearly embedded in the wording of the GDPR. Whether it is possible to make an ambiguous, multi-layered system understandable to the average person, and to craft juridical rights, remains to be seen. Clearly, judicial discretion remains key.

7. The effect of GDPR: Is it enough?

Although GDPR provisions have undoubtedly increased control over one's data, total control has not been achieved. Safari notes how hefty administrative fines "…discourage indifference and encourage compliance."[113] Article 83 sanctions require organisations in breach to pay up to €10,000,000 (EUR) or 2% of their annual turnover.[114] For example, British Airways faced a £183M fine in July 2019 when 500,000 customers' data was compromised.[115] Although the fines do not directly affect consumers, they do deter companies from infringing the Regulation and help ensure strict compliance. Scepticism remains over , in terms the Article 21 right to object. It may be difficult to identify just when personal data is being processed in the interests of the public and when such processing is "…necessary for the legitimate purposes of the controller or a third party."[116] Kuner et al frame GDPR as setting a global standard for data protection law but criticise its objectives. They hold that the legislation successfully addresses how data should be managed but fails to encourage increased minimisation of data usage.[117] It may be more beneficial to reduce the amount of data being processed to prevent unnecessary transactions instead of solely focusing on how it is processed. They propose an alternative system of monetary payments for services, using sensitive data: any data collected would be used for the service rather than having companies use it to generate profit (through advertising).[118]

Although this is appealing to users who may enjoy a degree of advert personalisation, it may be seen as paying to protect data privacy. This clearly goes against data subject rights and the entire aim of the GDPR. Kuner et al suggest that the GDPR may not be suited to the technicalities of automated data processing.[119] Samasiuk similarly argues that GDPR has seen multinational data privacy initiatives fall out of touch.[120] Consequently, such an initiative may

[113] B A Safari, "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection" *Seton Hall Law Review* (2017) 825
[114] GDPR Article 83 (4)
[115] BBC News, 'British Airways faces record £183m fine for data breach' BBC News (London 8 July 2019), <https://www.bbc.co.uk/news/business-48905907>
[116] Ibid 827
[117] C Kuner, F H Cate, O Lynskey, C Millard, N Ni Loideain and D J B. Svantesson, "If the Legislature Had Been Serious About Data Privacy…" *International Data Privacy Law* (2019) 75
[118] Ibid 76
[119] Kuner et al (n 117) 2
[120] V Samasiuk," When the GDPR is Not Quite Enough: Employee Privacy Considerations in Russia, Belarus and Ukraine." *Privacy Advisor* (2018) 9

need to be encouraged on a global scale. GDPR has at least created a template for other jurisdictions in terms of what effective data privacy laws should look like, even though there is little consensus yet on its effectiveness as a whole. Conflicting academic opinions on which sections need improvement will likely continue as societal and technological developments occur and case law unfolds. Though the GDPR has inconsistencies, there is always scope for refinement, given the rapidly advancing technology. It is important to accept the superiority of the GDPR in comparison to its predecessor and other multinational initiatives.

Blockchain technology merits mention here. It is a "…shared immutable digital ledger that records data (e.g. transactions, documents) packaged into identifiable blocks which are added to other existing blocks to create an interlinked chain on a decentralised network."[121] They are most commonly used through cryptocurrencies such as *Bitcoin*, creating permanent records designed to live outside governmental jurisdictions. Doubts arise over their compatibility with the Regulation, especially where they store personal information. Jan Philipp Albrecht (an MEP) notes that "certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subjects' rights] based on their architectural design."[122] On the authority of the Chief Finance Officer for *Bitnation*, John Mathews, the centralised services covered by the GDPR directly oppose the decentralised nature of Blockchain technology.[123] Despite its many benefits in the digital market, the 'openness, lack of permission and potential anonymity' creates tension between the technology and the Regulation.[124] As Wirth and Kolain further stress, on the surface blockchain technology appears to not process personal data at all.[125] The anonymity of the technology suggests that it operates beyond reach of GDPR. Personal data still seems to be identifiable, however. If a service is bought through cryptocurrency, the consumer may be identified via the provided address.[126] If so, the data is deemed 'pseudonymous' as it can be related back to the consumer with additional information. Tsakiridi insists that certain Blockchains may be able to work in tandem with the Regulation.[127] Their foundations resemble those set out in the GDPR, namely transparency and security. Though their encryption aspects remain confidential, the ledger itself upholds transparency. As blockchains appear tamper proof, they are less vulnerable to cyber-attacks.[128] Potentially, the

[121] S Tsakiridi, "Blockchain and the GDPR – Friends of Foes?" *Privacy and Data Protection* (2020) 3-6

[122] D Mayer, "Blockchain Technology is on a Collision Course with EU privacy Law" (*IAPP Privacy Advisor,* Feb 2018) < https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/> Accessed: 26.03.2020

[123] L Sayer, "The GDPR and Blockchain – can they coexist?" (*Carey Olsen,* May 2018) <https://www.careyolsen.com/articles/gdpr-and-blockchain-can-they-co-exist> Accessed: 26.03. 2020

[124] C Kuner, F Cate, O Lynskey, C Millard, N Ni Loideain and Svantesson, "Blockchain Versus Data Protection." *International Data Privacy Law* (Vol 8, 2018) 104

[125] C Wirth and M Kolain, "Privacy by Blockchain Design: A Blockchain-enabled GDPR-Compliant Approach for Handling Personal Data." *Reports of the European Society for Socially Embedded Technologies* (Vol. 2, 2018) 4

[126] Ibid

[127] Tsakiridi (n 121)

[128] Ibid, 5

structure of blockchains makes it impossible for them to be governed by one set rule and instead each case might be addressed on an ad hoc basis by a separate consortium.[129]

The issue of Brexit is also highly relevant, in terms of whether UK citizens will still be able to enforce rights gained under the GDPR. Initially, the UK government announced that they were "keen to secure the unhindered flow of data between the UK and the EU post-Brexit," which, at the time, meant that implementing the GDPR domestically would be the best way to achieve this objective.[130] Government confidence is evidenced by the enactment of the Regulation via the UK's new Data Protection Act (2018): at the point of withdrawal, UK laws should be compliant with those of the EU, facilitating continued exchanges of data. Writing prior to the Brexit Withdrawal Agreement, Murray cast doubt upon this: should the government choose a 'no-deal' Brexit, decisions might no longer be subject to the Commission or the European Court of Justice, raising a query over who might serve as ultimate adjudicator?[131] It would be foolish to assume however a continued application of the Regulation solely because of its domestic implementation in 2018.[132] There is nothing stopping the government from completely changing their data protection laws, which would affect consumer control. One saving grace, however, may be the requirement of adequacy under Article 45 (GDPR). Brexit will ultimately mean that the UK no longer part of the European Economic Area (EEA) - all data transactions will fall under restricted transfers between the EU and a 'third party' (the UK). Should the UK wish to proceed with 'unhindered' transfers of data to the EU, domestic legislation must provide an 'adequate' level of protection which subsequently involves a process of close legislative scrutiny carried out by the Commission.[133] It would be reasonable to assume that the easiest way to achieve this is to maintain the already implemented Act, thereby upholding GDPR rights.

Kuner et al suggest that compliance with the EU initiative may not be necessary, however. Instead, the UK's future data protection framework may be equally effective, if it were perhaps aligned with "…other international jurisdictions."[134] The ICO has acknowledged the appeal and quality of other data protection mechanisms, namely those of Australia, Indonesia, New Zealand and Canada,[135] although the UK's proximity to Europe might make this difficult. Patel and Lea have argued that their email system only operated due to free data transfers between Ireland and the UK.[136] Scrapping the GDPR could do more harm than good: its core

[129] Kuner et al (n 124) 104

[130] The Rt. Hon Matt Hancock, "The Data Protection Package" *EU Home Affairs Sub- Committee*, (1 February http://www.parliamentlive.tv/Event/Index/b3334d4c-93bf-4aca-9df5-666b7a72c06c> accessed 30.03.2020)

[131] A D Murray, "Data Transfers Between the EU and the UK Post Brexit?" *International Data Privacy Law* (Vol 7, 2017) 149 – 164

[132] Ibid 164

[133] GDPR Article 45 (2)

[134] C Kuner, D Jerker, B Svantesson, F H Cate, O Lynskey and C Millard, "The Global Data Implications of 'Brexit'" *International Data Privacy Law* (Vol 6, 2016) 168

[135] The Information Commissioner's Office, "Information Rights and Brexit Frequently Asked Questions" (ICO, v.2.3) <https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexitfaqs-v2_3.pdf> Accessed: 9th April 2020

[136] O Patel and Dr N Lea, "EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?" *UCL European Institute – Brexit Insights* (2019) 3

principles allow for "…the imbalance of power between the individual and the organisation to be rectified."[137] Much has already been done to uphold consumer rights and ensure company compliance with the Regulation. New, alternative data protection measures may cause mass uncertainty for organisations and further "… break the trust that individuals have in the regime." [138] According to ICO guidance, the GDPR remains in place during the current transition period and the government apparently intends to continue with application of the GDPR principles post-transition. In practice there should be little change: though there is no final proposal yet, the ICO identify the possibility of a 'UK GDPR,' a promising, if still uncertain outcome. [139]

8. Human Rights and Data Protection?

It is necessary to evaluate the existence or otherwise of a fundamental right to data protection. Article 8 of the European Convention on Human Rights (ECHR) enshrines the right to respect for private life. There is of course no explicit mention of protecting an individual's data, but several academics have added to the debate on whether Article 8's scope might include data protection, or whether privacy and data protection issues should instead be addressed independently. The *Rundfunk* case suggested that it would be reasonable to assume that data protection rights are subsumed into the wider right to privacy.[140] By interpreting the DPD in light of Article 8, the courts were able to identify the data breach as an infringement of a fundamental right, adding an extra dimension of data protection to the notion of privacy rights.

However, the same decision could well have been reached by applying the principles of the Directive. Lyskey notes that data protection as a fundamental right is more useful, giving consumers greater control rather than a mere qualified right to privacy: such control "…promotes the right to personality of individuals through informational self-determination and…reduces the information and power asymmetries which can have a negative impact on individual autonomy."[141] Tzanou outlines a 'separatist model,'[142] whereby a right to data protection will almost inevitably relate back to individual privacy. The two fulfil very different roles however, with privacy operating as a 'tool of opacity,' meaning it protects individuals from wrongful interference by authoritative bodies. As a 'tool of transparency,' data protection …is instead "directed towards the control and channelling of legitimate use of power."[143]

Data protection was elevated to the same status as the right to privacy in Article 8 of the Charter of Fundamental Rights.[144] Following the Treaty of Lisbon [2009], the right to protection of

[137] K Wynn, "Brexit – If It Ain't Broke, Why Break It?" *Privacy and Data Protection* (2019) 14
[138] O Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order" *International and Comparative Law Quarterly* (2014) 575
[139] ICO, n 136
[140] Case C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-4989
[141] Ibid 597
[142] M Tzanou (n 4) 4
[143] Ibid
[144] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, [2012] C 326/02

personal data was made binding within the EU's legal order. Despite this significant development in EU data protection law, the fundamental right was still considered a simple extension of the right to privacy. Tzanou suggests that for data protection to be a stand-alone right, it must be able to perform a dual purpose, by both awarding control and prohibiting power.[145] Arguably, the GDPR does this. Article 1 could be seen as promoting 'opacity' by implementing rules to protect "…natural persons with regard to the processing of personal data,"[146] whilst also defending the fundamental right granted by the Charter.[147] The GDPR presents its subjects with increased control over their personal data, satisfying Tzanou's 'transparency' tool requirement.

This is not to say that the fundamental right to data protection is omnipotent: the right can only be enforced within the EU which excludes other jurisdictions who likely have their own data protection laws. As Murray noted, post-Brexit, UK data consumers will no longer enjoy this fundamental right. Instead, "they will retain only the shadow of the right through the framework for data protection which will be found in the UK implementation of the GDPR."[148] Lacking the protection of both the EU Charter and the GDPR, UK data subjects will no longer have a consolidated enforcement mechanism, which is perhaps the backbone of the right. Regaining such legal protection would require the UK government to adopt their own, freestanding right to data protection.

9. **Conclusion**

The General Data Protection Regulation has completely reconceptualised the way in which data protection operates. It has shed light upon a complex area of law whilst strengthening the role of individual management and control of one's personal data. It has set a global data protection standard for other jurisdictions to perhaps emulate. With the continuously developing challenges of the digital age, data protection legislation had to be redesigned into a system that encompasses improved openness and consent. The GDPR significantly increases European citizens' control over their personal data in comparison with the earlier Data Protection Directive; the core principles of the Regulation have been designed with consumers in mind. The status of 'Regulation' has ensured that the legislation is being applied uniformly across the EU, requiring each member state to deliver domestic compliance. Instead of enforcement being limited to the authority of each member state, the increased territorial scope under the GDPR allows individuals to invoke their rights where their data is processed, even outside of the EU's territory.

[145] Tzanou (n 4) 99
[146] GDPR Art. 1(1)
[147] GDPR Art. 1 (2)
[148] Murray (n 131) 151

Additionally, widening the definition of 'personal data' means greater protection for data subjects and maintains the accountability of data controllers: penalties for failure to observe the provisions of the regulation further enhance consumer control. These are all crucial in terms of helping consumers gain a higher level of control over their own data, but what is most remarkable about the GDPR is the concept of data subject rights. The elevated importance of consent means that data subjects must be provided with an easily-understood description of how their data will be used so that they can make an *informed* decision on whether or not to proceed. As well as being able to control where their data goes, individuals can easily transfer it between processors or even request it to be erased entirely. Furthermore, depending on how the Regulation is interpreted, data subjects may also have the right to an explanation in respect of data that has been processed automatically. Such fluidity in data transfers considerably enhances consumer control over personal data.

That said, certain limitations continue to be apparent. The Regulation provides a framework for controls, but its efficacy depends in part upon the knowledge and understanding of the consumer. The complexity of the internet - and the invisibility of how data is processed and transferred - can make exercising complete control virtually impossible, especially given that data can be quickly and easily shared between multiple data controllers. Data profiling means that the preferences of consumers can be used to establish an intangible 'cyber identity' through which they can be manipulated and exploited without their knowledge or consent. Algorithmic accountability makes provision for consumers to challenge automated decisions, but the practical application of this right can only be achieved where a consumer can penetrate often complex and multi-layered decision-making systems. Given the fundamental status of the right to data protection under the EU legal order – and indeed the wider human right to privacy - the GDPR could perhaps have done more to address these shortcomings.

Future issues remain in need of resolution. It remains unclear whether the Regulation will be able to keep pace with the rapid development of new technologies including automated data processing: potential weaknesses in relation to Blockchains have already emerged. Given the relatively short life of the GDPR, interpretation of the Regulation is likely to occur via litigation: exceptions to the Right to be Forgotten, and the issue of where balance should be struck between consumer rights and fundamental rights, seem set to give rise to controversy. The full impacts of Brexit on data protection rules remains unknown: although the government may maintain the current framework in the short term, thereafter the data protection regime within the UK could be subject to amendment. The Regulation requires continuous scrutiny to ensure data protection principles are kept up to date so that fundamental rights are still being protected.

References

Adams Shoor, E "Narrowing the Right to be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation." *Brooklyn Journal of International Law* (2014) 487-520

Bhaimia, S "The General Data Protection Regulation: The Next Generation of EU Data Protection" *Legal Information Management* (2018) 21-26

Buttarelli, G "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard" *International Data Privacy Law* (Vol. 6, 2016)77-78

Calo, R "Digital Market Manipulation" *The George Washington Law Review* (Vol 4. 2014) 955-1051

Carey, P *Data Protection* (5th Edn. Oxford University Press, 2018)

Castelluccia C and Le Metayer D - European Parliamentary Research Service. "Understanding Algorithmic Decision- Makin: Opportunities and Challenges." *Panel for the Future of Science Technology* (2019)1-86

Chapman, C "A New Technological Age" *New Law Journal* (Vol 167, 2017) 18-21

Cohen, J E "Turning Privacy Inside Out" *Theoretical Inquiries in Law* (Vol 20, 2019)

Crabtree, A et al "Building Accountability into the Internet of Things: the IoT Databox Model" *Journal Of Reliable Intelligent Environments* (2018) 39-55

Dunphy-Moriel M and Dittel, A " Forget me Not: Limits to the Right of Erasure" *Computer and Telecommunications Law Review* (2020) 21-22

Eskens, S "Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should it?" *Institute for Information Law* (2016) 1-73

Goodman B and Flaxman, S "European Union Regulations on Algorithmic DecisionMaking and a 'Right to Explanation'" *AI Magazine* (2017) 50-57

Graef,I, M Husovec and N Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law" *German Law Journal* (2018)1359-1398

Gutwirth, S Y Poullet, P de Hart, C de Terwangne and S Nouwt, *Reinventing Data Protection?* (Springer, 2009)

Hörnle, J "Juggling more than three balls at once: multilevel jurisdictional challenges in EU Data Protection Regulation" *International Journal of Law & Information Technology* (Vol 27, 2019) 142-170

Information Commissioner's Office, "Guide to the General Date Protection Regulation (GDPR)" (ICO, 2019) <https://ico.org.uk/for-organisations/guide-to-dataprotection/guide-to-the-general-data-protection-regulationgdpr/principles/lawfulness-fairness-and-transparency/>

Information Commissioner's Office, "Information Rights and Brexit Frequently Asked Questions" (ICO, v.2.3) <https://ico.org.uk/media/for-organisations/documents/brexit/2617110/information-rights-and-brexit-faqsv2_3.pdf>

ITGP Privacy Team, EU General Data Protection Regulation (GDPR): An *Implementation and Compliance Guide* (2nd Ed. IT Governance Publishing, 2017)

Janal, R "Data Portability – A Tale of Two Concepts" *Journal of Intellectual Property* (2017) 59-69

Kaminski, M E "Right to Explanation, Explained" *Berkeley Technology Law Journal* (2019) 189-218

Kedzior, M "*GDPR and Beyond – A Year of Changes in the Data Protection Landscape of the European Union."* ERA Forum (2019) 505 – 509

Kuner, C F Cate, O Lynskey, C Millard, N Ni Loideain and D J B Svantesson, "Blockchain Versus Data Protection." *International Data Privacy Law* (Vol 8, 2018) 103- 104

Kuner, C F Cate, O Lynskey, C Millard, N Ni Loideain and D J B. Svantesson, "If the Legislature Had Been Serious About Data Privacy…" *International Data Privacy Law* (2019) 75-77

Kuner, C D Jerker, B Svantesson, F H. Cate, O Lynskey and C Millard, "Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?" *International Data Privacy Law (*Vol. 7, 2017) 1-2

Kuner, C, D Jerker, B Svantesson, F H Cate, O Lynskey and C Millard, "The Global Data Implications of 'Brexit'" *International Data Privacy Law* (Vol 6, 2016) 167-169

Lynskey, O "Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez" *Modern Law Review* (2015) 522 – 534

Lynskey, O "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order" *International and Comparative Law Quarterly* (2014) 569-597

Mayer, D "Blockchain Technology is on a Collision Course with EU privacy Law" (IAPP Privacy Advisor, Feb 2018) < https://iapp.org/news/a/blockchain-technology-is-on-acollision-course-with-eu-privacy-law/>

Mendoza I and Lee A Bygrave, "The Right Not to Be Subject to Automated Decisions Based on Profiling" University of Oslo Faculty of Law Legal Studies Research Paper Series No.2017-20 in T Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (Springer, Cham, CH 2017)

Murray, A D "Data Transfers Between the EU and the UK Post Brexit?" *International Data Privacy Law* (Vol 7, 2017) 149 – 164

Patel O and Dr N Lea, "*EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray?*" UCL European Institute – Brexit Insights (2019) 1-14

Politou, E, E Alepis and C Patsakis, "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions" *Journal of Cyber Security* (2017) 1-20

Reding V, "The Upcoming Data Protection Reform for the European Union" *International Data Privacy Law* (Vol.1, 2011) 3-5

Rempell, S "Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas" *Florida Journal of International Law* (Vol. 18, 2006) 807-842

Safari, B A "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection" *Seton Hall Law Review* (2017) 809-848

Samasiuk, V " When the GDPR is Not Quite Enough: Employee Privacy Considerations in Russia, Belarus and Ukraine." *Privacy Advisor* (2018) 1-10

Sayer, L "*The GDPR and Blockchain – can they coexist*?" (Carey Olsen, May 2018) https://www.careyolsen.com/articles/gdpr-and-blockchain-can-they-co-exist

Selbst AD and J Powles, "Meaningful Information and the Right to Explanation." *International Data Privacy Law* (Vol 4, 2017) 233-242

See Unity "*The Main Differences Between the DPD and the GDPR and How to Address Those Moving Forward*" (British Legal Technology Forum, 2017)

Tikkinen-Piri, C, A Rohunen, J Markkula, "EU General Data Protection Regulation: Changes and implications for personal data collecting companies," *Computer Law and Security Review* (Vol 34, 2018) 134-153

Tsakiridi, S "Blockchain and the GDPR – Friends of Foes?" *Privacy and Data Protection* (2020) 3-6

Tzanou, M "Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not so New Right" International Data Privacy Law (2013) 88-99

Van Ooijen I and H Vrabec, "GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective." *Journal of Consumer Policy* (2019) 91-107

Wachter, S, B Mittelstadt and L Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* (Vol 7. 2017) 76 – 99

Westin, A, *Privacy and Freedom* (Ig Publishing New York, 1967)

Wills, A "Richard Lloyd v Google LLC – Landmark Judgement in Representative Data Protection Action." *Entertainment Law Review* (2020) 52-56

Wirth C and M Kolain, "Privacy by Blockchain Design: A Blockchain-enabled GDPRCompliant Approach for Handling Personal Data." *Reports of the European Society for Socially Embedded Technologies* (Vol. 2, 2018)

Wynn, K "Brexit – If It Ain't Broke, Why Break It?" *Privacy and Data Protection* (2019) 11-14

Zalnieriute, W "Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement" *Modern Law Review* (Vol 81, 2018) 1046-1063