THE UK DATA PROTECTION ACT 2018

By Dr. Karen Mc Cullagh
Lecturer in Law, UEA Law School

I- BACKGROUND

With the UK on course to leave the European Union (on 29th March 2019, unless a later withdrawal date is agreed during trade negotiations) yet the General Data Protection Regulation (GDPR) scheduled to have direct effect in all member states beforehand i.e. from 25 May 2018, the UK Government introduced a data protection bill into Parliament, on 13th September 2017 to implement derogations in the GDPR into national law during the pre-withdrawal period and then retain the GDPR in UK law post-Brexit [1] The government's rationale for post-Brexit retention of GDPR provisions is that "We are leaving the EU and businesses need a single standard under which they can operate,"[2] so that data flows "*remain uninterrupted after the UK's exit from the EU [and EEA]*".[3] After much debate and some revision, it received royal assent on 23rd May 2018.

The Data Protection Act 2018 (hereafter the DPA) is the third generation of data protection legislation in the UK. It repealed and replaced the Data Protection Act 1998 that transposed the Data Protection Directive 95/46/EC into UK law, which had in turn replaced the Data Act 1984 which incorporated eight data protection principles arising from the Council of Europe Convention for the Processing of Personal data (hereafter referred to as Convention 108).

The DPA regulates the processing of individuals' personal data by the private and public sectors, law enforcement entities and intelligence service agencies It does so by providing rules concerning general data processing, law enforcement data processing, data processing by the intelligence services, and regulatory oversight and enforcement by the national supervisory authority - the Information Commissioner's Office (ICO).

II-SCOPE & STRUCTURE OF THE ACT

The DPA, subject to minor exceptions, extends and applies to the whole of the UK.[4] This complex and lengthy (339 pages) Act is set out in seven parts:

Part 1 explains the structure of the Act and contains some general definitions. **Part 2** has three chapters, the first of which contains definitions and general material. Chapter 2 (which must be read alongside the GDPR) sets out national derogations from the GDPR, such as the definition of public authority and public interest, the age of consent for children using information society services, a system for authorising certification providers, and safeguards for processing for archiving, research and statistical purposes. The derogations will be discussed in more detail below. Chapter 3 applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply including the processing of unstructured manual files by public authorities but excluding law enforcement and intelligence agency (e.g. GCHQ) processing.

Part 3 is divided into six Chapters. This part transposes the Law Enforcement Directive (LED) into UK law. It applies to all processing for law enforcement purposes by a defined list of "competent authorities" listed in Schedule 7 that includes organisations such as Government departments, Fraud Office, Police, Probation, Youth Offending Teams etc.

Part 4 provides a code of personal data processing for the intelligence agencies in six chapters. It draws from the modernised Convention 108. The rules in this Part contain predictably wide exemptions for national security processing.

1 Data Protection Bill [HL] 2017-19, <https://services.parliament.uk/bills/2017-19/dataprotection.html>
2 DCMS, A New Data Protection Bill: Our Planned Reforms, A Statement of Intent, (7 August 2017), <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf> 14.
3 Ibid, 24.

4 Data protection is not a devolved matter in Scotland, Wales, or Northern Ireland.

THE UK DATA PROTECTION ACT 2018 by, *Dr. Karen Mc Cullagh*

Part 5 contains provisions to continue the existence of the role of the ICO and its functions.

Part 6 deals with enforcement of the data protection legislation i.e. the ICO's powers to issue enforcement notices and penalties.

Part 7 of the Act contains miscellaneous provisions such as order-making powers.

Most provisions in the DPA 2018 came into force on 25th May 2018 to coordinate with the General Data Protection Regulation (GDPR) becoming directly applicable in EU member states.[5] When the UK leaves the EU, the GDPR will be incorporated into the UK's domestic law under the European Union (Withdrawal) Bill, currently before Parliament.[6]

III-GENERAL OBSERVATIONS

The DPA is highly 'conservative,' departing in approach and terminology from the previous Act as little as possible. This is understandable in light of (i) the short timescale available before the GDPR came into effect and the LED had be transposed and (ii) the need to be mindful of 'adequacy' requirements as part of the Brexit process. Although the post-Brexit EU-UK relationship has not yet been finalised, it is highly likely that the UK will become a 'third country' for data protection purposes (unless it becomes an EEA country) and be obliged to seek an adequacy decision from the European Commission in order to facilitate unimpeded personal data from the EU to the UK. Retaining the Data Protection Act 1998 was not an option because the European Commission had instigated infringement proceedings against the UK government for failure to properly implement 11 articles in the Directive into the DPA 1998 - a clear sign that the UK's Data Protection Act 1998 would not be found to provide an adequate level of data protection.[7]

Therefore, the easiest way for the UK to ensure an equivalent level of protection was by inserting terms that are wither identical to, or else closely mirror, provisions in the GDPR in the DPA. Even so, there may be other barriers to an adequacy decision, a point that will be returned to later.

IV-UNCONTENTIOUS ASPECTS

Part 2, Chapter 2 (and Schedules 1-3) of the DPA sets out derogations permitted in the opening clauses of the GDPR. The UK Government has used these derogations to ensure close alignment with the approach adopted under the previous data protection act or other existing laws. A few of the more notable derogations and powers are set out below:

A-Public authority & public task: definitions and exemptions

The GDPR contains numerous references to public authorities e.g. when stipulating, in Art 37, that such bodies need to appoint a Data Protection Officer, and when stipulating in Art 6(1)(f) that public authorities processing personal data in the performance of their public tasks cannot rely on 'legitimate interests' as the lawful basis for processing. As the terms 'public authority' and 'public body' are not defined in the GDPR, the DPA adopts in section 7 the definitions in the Freedom of Information Act 2000 and its Scottish equivalent, the Freedom of Information (Scotland) Act 2002, as well as bodies specified by the Secretary of State, subject to two qualifications. First, public authorities are only to be treated as public authorities for the purposes of the GDPR when they are carrying out a task in the public interest or in the exercise of official authority vested in it. Second, parish councils,

5 By virtue of s 212 of the Data Protection Act 2018 and the Data Protection Act 2018 (Commencement No1 and Transitional and Savings Provisions) Regulations 2018 (SI 2018, No. 625), some provisions will come into effect on 23rd July. Of note is that provisions brought into force requiring the ICO to prepare a Code of Practice (e.g. the age verification code under section 123), include an obligation to consult. Following consultation and preparation of a Code of Practice, the ICO is required to lay the code before Parliament for a period of 40 days to fulfill the procedural approval process. Consequently, there is likely to be a delay in the introduction of Codes of Practice with the effect that they are unlikely to be in place by 23rd July 2018. Furthermore, there are a few provisions that are not in force and not subject to any commencement provisions: Schedule 6, para 62 (which appears to make a technical amendment to the GDPR in respect of Art 89, (safeguards and derogations) relating to processing for archiving purposes etc.); Part 4 (Intelligence Service processing), ss 93 (right to information), 102 (general obligations of the data controller), 103 (data protection by design), 104 (joint controllers), 105 (processors), 108; (communication of a personal data breach) a and Schedule 19 (minor and inconsequential amendments), paras 76, 201, 222 1nd 227 (which appear to relate to (i) investigatory powers and (ii) social workers).

6 Clause 3.

7 C Pounder, 'European Commission Explains Why UK's Data Protection Act is Deficient' <http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html>; C Pounder, 'Copy Correspondence Between Dr Chris Pounder and EU Commission & Ombudsman' <http://amberhawk.typepad.com/files/dp_infraction_reasons.pdf>; C Pounder, 'European Commission Raises Infraction Threat to UK on Failing to Implement Directive 95/46/EC Properly via the Data Protection Act' <http://amberhawk.typepad.com/amberhawk/2014/10/european-commission-raises-infraction-threat-to-uk-on-failing-to-implement-directive-9546ec-properly.html>.

THE UK DATA PROTECTION ACT 2018 by, *Dr. Karen Mc Cullagh*

community councils, and similar bodies are specifically excluded in section 7(3) from the definition. The government's rationale for exempting these bodies is that they these bodies are very small in terms of personnel, budget, and the volume of personal data they process such that the additional safeguards that public authorities normally have to apply would represent a disproportionate burden.[8] Consequently, parish councils and other exempt bodies do not need to appoint a data protection officer and can rely on legitimate interests as their lawful basis for processing personal data.

B-Child's consent in relation to information society services

Section 9 sets the age at which a child can give consent to the processing of data for the purposes of the provision of information society services at 13 years old. On this point, the Government seems to have listened to concerns from children's charities, who encourage respecting the agency of young people and who considered the prospect of 14 and 15-year-olds needing parental consent for much of their online activity as a backwards step.

The Government favoured an approach in which protections for young people derive from the systems themselves being designed securely, rather than reliance on parental consent. This approach will pose a big challenge for online operators as they will be obligated to set up parental consent systems when they are needed, and have a way of showing that they have implemented appropriate techniques to verify age (which, as I reported in a previous paper is difficult when children are au fait with techniques for bypassing age verification mechanisms and obtaining parental consent).[9]

C-Continued registration with and payment of fees to the ICO

Although the removal of data protection registration requirements across the EU was a hailed as a positive provision in the GDPR, the obligation to register with (also known as notification) and pay a fee to the ICO has been retained in a separate law, the Data Protection (Charges and Information) Regulations 2018.[10] Different levels of fees (ranging from £40 to £2,900 per annum) are to be levied depending on the size of the data controller.

D-Stronger ICO investigatory & enforcement powers

In the wake of the Facebook-Cambridge Analytica data scandal (which involved the collection by Cambridge Analytica of the personal data of up to 87 million Facebook users in an attempt to influence voter opinions), the ICOs efforts to investigate and enforce were hampered by provisions in the Data Protection Act 1998 that required data controllers to be given seven days of notice in writing of the intended search, and be given an opportunity to argue in court against the granting of warrant.

The DPA has enhanced the powers of the ICO through the introduction of an obligation for data controllers to respond to urgent information requests from the ICO within 24 hours,[11] the ability to obtain court orders to require disclosure when data controllers refuse to hand such information over,[12] as well as the introduction of an offence for destroying, falsifying or concealing information.[13]

Also, whilst the maximum fine that the ICO can impose has been increased from £500,000 to €20m or 4% of worldwide annual turnover (with the penalty in sterling to be determined by applying the spot exchange rate set by the Bank of England on the date on which the penalty notice is issued,[14] it is important to note that the ICO views itself as a 'proportionate regulator' and has sought to reassure data controllers that maximum penalties will only be issued in respect of the most serious breaches.

Nevertheless, the ICO has also stated that in its opinion a more effective tool in its armoury may be its ability to prohibit data controllers and data processors from processing personal data. In effect, it has issued a warning to 'big players' that a potential fine should not be viewed a 'worthwhile business cost.' Rather, the ICO's power to make them cease personal data processing activities should give them pause for thought and be an effective compliance 'stick' in situations where one is needed, particularly when it could have knock on implications in terms of failing to meet corporate governance requirements or the triggering of a report to a stock exchange.

8 Data Protection Act 2018, Explanatory Notes, <http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf>, para 23.
9 K Mc Cullagh, (2016) The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?, in Data Protection, Privacy and European Regulation in the Digital Age. Forum Iuris, ISBN 978-951-51-2530-9.

10 The Data Protection (Charges and Information) Regulations 2018 were made under a power in the Digital Economy Act 2017.
11 Section 142.
12 Section 145.
13 Section 148.
14 Section 157(7).

THE UK DATA PROTECTION ACT 2018 by, *Dr. Karen Mc Cullagh*

V-CONTENTIOUS ASPECTS

Not all provisions in the DPA have been welcomed. At least seven were the subject of criticism during the legislative process and some provisions continue to be considered controversial for the reasons set out below:

A-Journalism exemption & Leveson inquiry Part 2

A significant amount of time was spent debating proposed amendments scheduled by opposition parties relating to press regulation – i.e. on commencing part 2 of the Leveson inquiry and bringing section 40 of the Crime and Courts Act 2013 into force. Part 2 of the Leveson Inquiry had been intended to address '*the extent of unlawful or improper conduct within News International and other media organisations, and collusion between the police, press and politicians*.'[15] It was postponed in 2012, to avoid prejudicing the large-scale police investigations into phone hacking and corrupt payments, which were then ongoing. Section 40 of the Crime and Courts Act 2013 would have made news publishers who were not subject to a Government-approved regulator, liable for the costs of defamation, privacy, and harassment claims, regardless of whether they won or lost. The proposed amendments were ultimately defeated and s 40 of the 2013 Act will now be repealed at the earliest opportunity.

Instead, the journalism exemption available under the Data Protection Act 1998 has been reproduced and its scope widened. Under 32 of the Data Protection Act 1998, a data controller processing for two or more substantive purposes, including for journalism, was on the face of the legislation precluded from relying on the exemption. By contrast, Schedule 2, part 5, para 26(3) is wider as it stipulates that the disapplication of certain GDPR provisions for journalists will apply '*to the processing of personal data carried out for the special purposes, whether or not the data are being processed for a second or ancillary purpose*.'

Also, although the DPA new criminal data offences, explicit journalism public interest defences have also been introduced.[16] When forming a belief that publication is in the public interest, a data controller must have regard to relevant codes of practice, namely the BBC Editorial Guidelines, the Ofcom Broadcasting Code and the Editors' Code of Practice.[17]

Significantly, the ICO has been granted powers and responsibility to encourage media compliance with data protection laws, including periodic review and reporting on compliance, an obligation to issue guidance to individuals on seeking redress against media organisations and creation of a code of practice for media organisations on data protection compliance to be approved by Parliament.[18] In addition, the Secretary of State must report every three years on the effectiveness of the media dispute resolution procedures, including under the Editors' Code of Practice.[19]

Thus, whilst the correct balance has arguably been struck between regulation and oversight to the media and its compliance with data protection legislation, the provisions in the DPA are, nevertheless, unlikely to appease those calling for Part 2 of the Leveson Inquiry to be conducted, as they contend that '*the government has surrendered to press lobbying, betrayed promises made to the victims of phone-hacking and undermined the public interest, in failing to conduct Part 2 of the Leveson Inquiry*.'[20]

B-Profiling by political parties

Despite the Facebook-Cambridge Analytica data scandal, the DPA contains a provision that permits political parties to process personal data 'revealing political opinions' (without the individual's consent), for the purposes of their political activities, [21] with "democratic engagement" listed as an example of processing activities that can be undertaken lawfully in the public interest.[22]

Privacy International have expressed dismay that 'There is nothing in the provision to prohibit delegation of such activities to a third party specialising in profiling.' They are particularly concerned as 'modern technologies make it possible to infer political inclinations of people from a wide variety of sources of information.'[23] Consequently, Privacy International contend that the provision is open to abuse and will facilitate targeted and exploitative political advertising. Accordingly, they wrote to the main UK political parties seeking to elicit a

15 Leveson Inquiry, Terms of Reference, Part 2, <http://webarchive.nationalarchives.gov.uk/20140122144942/http://www.levesoninquiry.org.uk/about/terms-of-reference/>
16 Sections 170-171.
17 Schedule 2, part 5, para 26(5).
18 Section 178.
19 Section 179.
20 S Barnett, The government scuppers Leveson Part 2: is Britain's press undermining democracy, Inforrm Blog, (22nd May 2018), <https://inforrm.org/2018/05/22/the-government-scuppers-leveson-part-2-is-britains-press-undermining-democracy-steven-barnett/>
21 Schedule 1, para 22.
22 Section 8 (e).
23 Privacy International, 'UK Data Protection Act 2018 – 339 pages still falls short on human rights protection,' (13th June 2018) <https://privacyinternational.org/blog/2074/uk-data-protection-act-2018-339-pages-still-falls-short-human-rights-protection>.

THE UK DATA PROTECTION ACT 2018 by, *Dr. Karen Mc Cullagh*

public commitment not to use profiling and targeting techniques in future political campaigns.[24] At the time of writing this working paper no political parties had responded to their request. It remains to be seen whether any lessons will be learned (and implemented) from the Cambridge Analytica scandal when the ICO investigation of the matter is completed.

C-Confidential References

The DPA allows confidential references to be kept secret in all circumstances, not just in the hands of the employer/giver of the reference (under the previous data protection Act employees could obtain such references by submitting a subject access request to a prospective employer, though not their current employer/reference provider as they were exempt from the subject access provision).[25] The DPA also gives an exemption from the right to be informed under Article 13 and 14 of GDPR i.e. the need to mention it in a privacy notice. The change will come as a surprise to many, especially as it was passed without any debate or discussion of the rationale for doing so.

Significantly, the exemption could very well mean that the UK is in breach of Article 8 of the European Convention of Human Rights 1950 as the exemption mirrors the facts in the case of *Gaskin v UK* (1989).[26] Therefore, it is highly likely that this provision will be challenged in the near future. Indeed, it may also represent a stumbling block to an adequacy decision, a point that will be discussed further below.

D-Henry VIII clauses (delegated powers)

The Act gives wide powers to the Secretary of State alter the application of GDPR, including conditions for processing sensitive personal data. The government has justified this approach (which bypasses effective parliamentary scrutiny) on the basis that it will provide necessary 'flexibility to manage unforeseeable circumstances (citing the decision by the Home Secretary to establish the Hillsborough Independent Panel to investigate the circumstances in which multiple fatalities occurred at a football stadium, as an example).[27]

E-No Collective redress mechanism

Despite many calling for the UK to implement the collective redress mechanism set out in Art 80(2) of the GDPR, the UK government decided not (at this stage) to allow qualified non-profit organisations to take independent action when they consider that there has been a failure to comply with the DPA. There is some room for optimism in relation to this provision though as the Government made a small concession in the form of an agreement to review this provision within 30 months of the commencement of this section.[28]

F-Immigration exemption

Schedule 2, part 1, paragraph 4 introduces a new exemption which restricts the application of certain GDPR provisions to personal data processed for the purposes of the maintenance of effective immigration control, or the investigation or detection of activities that would undermine the maintenance of effective immigration control, to the extent that the application of those provisions would be likely to prejudice those purposes.

Specifically, it removes most of a data subject's rights, including the right to access, right to erasure, right to restrict processing, right to object to processing); and all the principles in Article 5 of the GDPR (which require that processing must be lawful, fair and transparent, accurate, adequate, for explicit and legitimate purposes, processed in a manner that is secure, and limited to the specific original processing purpose).

The immigration exemption was introduced despite strong criticism from the ICO who observed that "If the exemption is applied, individuals will not be able to access their personal data to identify any factual inaccuracies and it will mean that the system lacks transparency and is fundamentally unfair,"[29] and submissions by the Deputy Counsel to the Joint Committee on Human Rights (JCHR) who queried "why immigration control requires exemptions from fundamental principles such as lawfulness, fairness and accuracy in order to maintain its effectiveness", and further contended that "it is arguably disproportionate to extend such restrictions to immigration control, particularly so in relation to lawful immigration."[30]

24 Privacy International, 'Privacy International asks major UK political parties to commit to not using legal loophole to target voters in forthcoming elections,' (15th May 2018) <https://privacyinternational.org/press-release/2032/privacy-international-asks-major-uk-political-parties-commit-not-using-legal>
25 Schedule 2, Part 4, Para 22.
26 *Gaskin v. UK*, Application no. 10454/83); 7 July 1989 <https://hudoc.echr.coe.int/eng#{"dmdocnumber":["695368"],"itemid":["001-57491"]}>
27 Data Protection Act 2018, Explanatory Notes, para 27.
28 Section 187.
29 ICO Briefing (2017), 'Data Protection Bill, House of Lords Report Stage –Information Commissioner's briefing – Annexx II,' <https://ico.org.uk/media/about-the-ico/documents/2172865/dp-bill-lords-ico-briefing-report-stage-annex-ii-20171207.pdf>.
30 Deputy Counsel, 'The Human Rights Implications of the Data Protection Bill', 6 December 2017, <https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf>.

Observers were surprised at this course of action, not least because the Government was already 'under fire' for the way it had 'mishandled' immigration data relating to the Windrush Generation (a term used to refer to individuals who moved from the West Indies to the UK between 1948 and 1971 at the express invitation of the UK Government who offered them indefinite leave to remain status for helping to rebuild the UK's economy post-WWII). The Home Office had disposed of 'landing card' that were often a key piece of documentary evidence proving their right to remain. Naturally, there are clear parallels between the position of the Windrush Generation and the 3 Million EU citizens currently resident in the UK whose status may be questioned when the UK withdraws from the EU. Unsurprisingly, there are plans to seek a judicial review of this element of the DPA.[31] It also has a strong potential to impact negatively on any post-Brexit adequacy decision that that UK may seek from the EU Commission in respect of EU-UK personal data transfers.

G-Intelligence Agencies

Despite Privacy International and others making submissions during the legislative process requesting that similar safeguards by imposed on intelligence agencies as apply to law enforcement bodies, the Government declined to introduce such safeguards, with the result that the DPA allows for non-transparent, unfettered and unaccountable intelligence sharing.

Privacy International assert that the DPA fails to meet the standards required by the Council of Europe modernised Convention 108, which the Act purports to follow.[32] If the EU share that view, it may be a barrier to obtaining an adequacy decision to facilitate EU-UK personal data transfers post Brexit.

VI-CONCLUDING REMARKS: A FINAL WORD ON 'ADEQUACY'

The UK Government is to be commended for taking the opportunity to strengthen the powers of the ICO in the DPA. Although this is positive, the DPA does contain problematic provisions. Already there are plans afoot to challenge the immigration exemption in the courts.

The UK Government intends to incorporate the GDPR into domestic law when it ceases to be a member of the EU despite not being legally obliged to do so when it becomes a third country. The rationale for doing so is the economic value of EU-UK personal data transfers. The UK economy is largely service based (service industries account for approximately 78% of the UK's Gross Domestic Product (GDP),[33] and personal data processing underpins these service industries. The UK will seek to maintain a trading relationship with the EU post-Brexit as the EU is the world's largest trading bloc and the world's largest trader of manufactured goods and services. [4]

In order to maintain unimpeded EU-UK personal data transfers, an adequacy decision will need to be obtained.[34] The EU Commission is the body responsible for making adequacy decisions. It will do so by conducting an abstract assessment of the UK's legal and administrative system in relation to the protection of personal data.[35] If satisfied, it will issue a legally binding 'adequacy decision' confirming that the UK offers adequate level of protection, so that transfers of personal data are lawful. If the Commission found that the level of protection in the UK was inadequate, data transfers could be halted. Thus, the refusal of an adequacy decision could have an economically damaging impact on the UK – a fate that the UK will surely seek to avoid. This will require the UK to not only amend the immigration and intelligence services provisions in the DPA but other legislation e.g. the Investigatory Powers Act 2016, (which is beyond the scope of this working paper).

It is highly likely that some Brexiteers[36] will complain about and resent the continuing influence of the EU in relation to UK data protection law. However privacy and data protection advocates are likely to extol the UK's post-withdrawal compliance with the GDPR as early evidence of how influential and effective the 'gold standard' protections in the GDPR will be in raising the standards of privacy and data protection across the globe.

31 Leigh Day, 'Rights groups to take Government to court over immigration exemption,' <https://www.leighday.co.uk/News/News-2018/May-2018/Rights-groups-to-take-Government-to-court-over-imm>

32 Privacy International, 'UK Data Protection Act 2018 – 339 pages still falls short on human rights protection,' (13th June 2018) <https://privacyinternational.org/blog/2074/uk-data-protection-act-2018-339-pages-still-falls-short-human-rights-protection>.

33 ONS, Statistical Bulletin: Index of Services, April 2016.

34 For a discussion of why consent, model clauses, and binding contract rules would not be suitable alternatives for EU-UK personal data transfers, see K Mc Cullagh, (2017) Brexit: Potential Implications for Digital and 'Fintech' industries, in International Data Privacy Law 7 (1) pp. 3-21.

35 GDPR, Art 45.

36 Those supporting Brexit are sometimes referred to as "Brexiteers."