An adequacy determination does not resolve the lower standard of data protection in the UK.

Just published on https://amberhawk.typepad.com/

In the next three weeks, there will either be a trade agreement with the European Commission (EC) or no trade agreement. As a sophisticated Barnsley fan, I have unshakeable faith in my abilities to recognise that one of these two outcomes will be correct.

If there is a trade agreement, I suspect the EC will chuck in an adequacy agreement with the UK with the caveat that it is subject to review by the Council of Ministers, European Data Protection Board and European Parliament. Such a review is likely to consider the problems I have identified below.

In effect, any adequacy agreement kicks the can (i.e. the problem of transfers of personal data from the EU to the UK and vice-versa) down the road for at least three years. That is until a privacy NGO completes its long march through the legal institutions to the CJEU and challenges the EC's determination of adequacy.

This blog lists a baker's dozen of longer-term data protection issues that afflicts the UK's Data Protection regime. An adequacy determination for the UK is unlikely to fix many of these issues; it just kicks them into touch.

However, what I can say is that when Ministers say "*we have a high standard of data protection*" – compared with European Union the answer is "***probably NO***" – compared with everywhere else that has a data protection law, the answer is likely to be "***probably YES***".

Anyway, this is a long blog – so you might want to prefer to download it as a pdf (here).

Problem 1: UK's lack of commitment to European privacy standards

The UK Government has a fragile relationship with the European Convention of Human Rights (ECHR) and, as a result, data protection. Divergence from European privacy norms has been signalled for more than a decade; for example:

- **The Conservative Manifesto of 2010** referred to replacing Human Rights Act with UK Bill of Rights. However, Recitals 1 to 4 of Directive 95/46/EC make **explicit** reference to the importance of safeguarding the "*fundamental rights of*

individuals" especially that expressed by Article 8 ECHR ("*right to respect for private and family life*…"). So as early as 2010, this Manifesto is describing the desirability of divergence from the data protection standards established by the Directive.

- **The Conservative Manifesto of 2017** put the "*right to data protection*" under threat because it stated: "*We will not bring the European Union's Charter of Fundamental Rights into UK law."* Recital 1 of the GDPR states that "*The protection of natural persons in relation to the processing of personal data is a fundamental right*" and that "*Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') …. provide that everyone has the right to the protection of personal data concerning him or her*". Hence, implementing the GDPR is seen as implementing part of this "*right to data protection*"; yet here is a clear statement of intent from the UK that this won't happen.

- **The Conservative Manifesto of 2019**. There is reference to "*updating*" the Human Rights Act and reducing the ability for Judicial Review (e.g. in cases such as the Judicial Review of the immigration exemption in the DPA2018 or the use of facial recognition CCTV by the Police).

Hence the Prime Minister's Written Statement of 3rd February 2020 (that "*The UK will in future develop separate and independent policies in areas such as … data protectio*n…") comes as no surprise. It's another signal that existing policy, first elucidated in 2010, that suggests that significant divergence in data protection/human rights from European norms is more than possible.

The history explains why the EC is concerned; in March 2020, the *Independent* Newspaper reported the EC lead negotiator telling reporters that "*the UK informs us that they do not wish to commit formally to applying the European Convention on Human Rights*".

Problem 2: UK's version of the GDPR can be changed on a whim

Powers in the European Withdrawal Act (EWA) 2018 have been used to create a UK version of the GDPR (the "UK_GDPR"). These EWA powers can also permit major divergence from the GDPR and vary **any** GDPR obligation (e.g. vary Principles, definitions, rights, security and transfer arrangements) without recourse to Parliamentary scrutiny.

By contrast, modifications by Member States to the GDPR is limited to about 50 Articles which are subject to review by the European Data Protection Board (which is tasked with harmonising approaches to the GDPR across Member States).

For example, when the UK becomes a fully-fledged Third Country outside the Withdrawal Agreement (expected January 1st next year), the UK Government has signalled that Gibraltar will become "adequate" for data protection transfers from the UK (see references). By contrast there is no adequacy determination for transfers to Gibraltar from the EU under the GDPR.

In extreme, the UK could use adequacy arrangements as a bargaining chip in future trade negotiations (e.g. "*If you drop your chlorinated chickens proposal we can offer an adequacy agreement?*") whereas the European Commission has a specific adequacy procedure to follow (e.g. involving the European Data Protection Board).

The major problem the EU has, in general, is that if there is an adequacy agreement with the UK, what is to stop the UK fundamentally modifying the content of the UK_GDPR after the ink on that agreement has dried?

Afterall, if the Government is willing to breach International Treaties (as per the Internal Markets Bill), varying an adequacy agreement should be "guilt free".

Problem 3: The Independence of the ICO is at risk

Changes made under EWA powers directly threatens the independence of the Information Commissioner's Office (ICO). For instance, the provision in Schedule 1, paragraph 45(3) of the Brexit DP Regulations (see references) has removed the word "*independent*" from Article 51(1) of the GDPR, so the independence of the ICO for the UK is no longer a legal requirement.

The next provision (Schedule 1, paragraph 45(4) of the Brexit DP Regulations) removes the obligations in Article 52(4) to 52(6). These Articles effectively require the UK Government to provide for adequate resources to be allocated to the ICO, for the ICO to choose his own staff and the obligation not to starve the ICO of funding.

Now I am not saying that this lack of independence or funding will happen; however, we now have to trust our politicians that it won't happen.

Problem 4: Data Subjects and legitimate interests at risk

The general protection of data subjects also risks being diminished. This reduction in protection arises from the UK's Government's intent to discount the interpretative impact of the Recitals to the GDPR and in its UK variant (the UK_GDPR).

Many of these Recitals describe how the Article is supposed to work. For example, marketing people should note that Recital 47 goes (legitimate interest for marketing) but then so does Recital 32 (pre-ticked opt-in boxes are not consent).

In summary, any interpretation of the UK_GDPR, based on the content of the Recitals of the GDPR, is unlikely to be enforceable in the UK (unlike in Member States under the GDPR itself). This was signalled by Government Ministers in Parliament during the passage of the Data Protection Bill:

> *"….the Recitals to the GDPR do not have normative effect—they are more akin to Explanatory Notes—and there is no requirement for the UK to enshrine them in legislation …. It is important to say that Recitals do not contain substantive law, nor can they override the express language of a regulation*" (Col 1189,30 Oct 2017, , Lords Hansard; Baroness Chisholm of Owlpen).

Problem 5: A "hostile environment" for Europeans in the UK

The immigration control exemption (DPA2018: Schedule 2, paragraph 4) makes it easier for the UK to apply its "*hostile environment*" policy to EU nationals resident in the UK. This exemption did not feature in the DPA1984, nor in the DPA1998, and applies to the processing of personal data for administrative immigration matters that do not concern to crime, tax or national security.

This controversial exemption has been subject to Judicial Review organised by the Open Rights Group. Although the lower courts decided the exemption was lawful, that decision is subject to an Appeal to the higher Courts.

Problem 6: In breach of an A.8 ECHR Judgement?

The subject access exemption relating to confidential references in the field of employment and education (DPA2018: Schedule 2, paragraph 24) could place data subjects at a disadvantage when they seek jobs or educational opportunities in post Brexit UK (as compared with mainland Europe).

This exemption extends to the right of access (A.15) to the reference and information about the context of processing (A.13 & A.14); it applies to both the sender and

recipient of the reference. The provision allows, for example, for one organisation to send a secret reference to another organisation about a prospective employee.

The DPA1998 version of this exemption (in Schedule 7, paragraph 1) was more compact: it only applied to the sender of the reference and did not exempt the transparency arrangements – so the existence of the reference could not be kept secret.

The more comprehensive DPA2018 exemption is inconsistent with the ECHR judgment in *Gaskin v UK: 1989 (12 EHRR 36)*. In *Gaskin*, the Court recognised that confidentiality is necessary for the protection of confidential personal data provided by Third Parties to an organisation, but stated there needed to be a counterbalance in the form of an independent check on the content of a particular reference when this was needed.

Under the DPA1998, that independent check was undertaken by the ICO. That is why the exemption only applied to the sender of the confidential reference; the Recipient of the same reference, on subject access, had to negotiate the balancing tests of Sections 7(4)-7(6) which could be challenged by the data subject to the ICO (who could then independently assess the content – thus complying with *Gaskin*).

The DPA2018 exemption thus reduces the protection for data subjects when personal data are contained in secret confidential references used for employment and educational purposes**.**

Such references can be absolutely exempt from the right of access and the data subject might not know they exist. That is why I think the UK has resiled from its implementation of the *Gaskin* ECHR Judgement.

Problem 7: In breach of CJEU decision?

The exemption for exam scripts (DPA2018: Schedule 2, paragraph 25) has been fashioned without regard to a CJEU decision in the case of *Peter Nowak (case C434/16*).

The Court in this case stated that a candidate could have the right of access to these personal data on the script but not the questions as "***an exam question would <u>NOT</u> constitute personal data"*** (my emphasis of paragraph 58 of the judgment).

Yet the official explanation for this exemption in the DPA2018 (see reference*)* states the complete opposite: the script is exempt from access because "…*This is necessary*

to protect the confidentiality of the questions so that awarding organisations can re-use questions where appropriate".

Ooops! The exemption in the DPA2018 is not needed for the reasons expressed by the UK Government.

Problem 8: Spooky issues

You are probably aware of this one, so I won't spend ages on it. The processing of personal data by UK intelligence agencies, especially its controversial bulk collection of communication data has been well litigated.

In particular, the indiscriminate bulk collection of communications metadata ("*related communications data*") from selected "*bearers*" in the underseas communication cables would appear to be contrary to principles established by the European Court of Human Rights (*Big Brother Watch v. the UK*) and the CJEU (*Tele2/Watson, Digital Rights, Schrems II, Privacy International and La Quadrature du Net*).

Problem 9: "Psst – wanna exemption from the data subject rights?"

There is an ability for UK ministers to implement exemptions in the DPA2018 that are not implemented in any other European data protection law. These could reduce the data protection rights of data subjects resident in the UK.

A.23(1) of the GDPR has been generously used by the UK Government to create 34 pages of exemptions in the DPA2018, several of which are new to the UK's data protection regime. More exemptions could follow, especially if they are introduced on "*general public interest*" grounds as specified in A.23(1)(e).

Opposition to these exemptions is likely to take the form of a NGO taking a Judicial Review to assess whether any particular exemption is lawful (i.e. "*necessary and proportionate*" as required by A.23(1), as with the immigration exemption described in Problem 5 above).

However, this prospect could be diminished: the Government are reviewing Judicial Review as the Government claims that it is being used excessively to interfere with Government Policy.

Problem 10: "Psst – wanna process sensitive stuff"?

Ministers have used the flexibility in A.9 & A.10 of the GDPR to expand the processing of special category of personal data or to authorise wider processing of criminal offence personal data. Sixteen pages of the DPA2018 (Schedule 1) text are already devoted to this topic.

Specifically, there are about 30 additional conditions or authorisation already in Schedule 1 and a further 10 conditions in Article 9 of the GDPR; this means that most controllers will look to Schedule 1 for the relevant condition or authorisation when processing these sensitive kinds of personal data.

It is very likely that Schedule 1 permits the processing of these sensitive personal data in circumstances not implemented in other European data protection laws.

Problem 11: "Psst – wanna share personal data?"

The extension of the A.6 lawful public task basis to an unlimited, non-exhaustive public task, legal basis by Section 8 of the DPA2018 could permit an extensive public task justification for data sharing between diverse public sector bodies (e.g. as envisaged by the Digital Economy Act 2017).

It is noteworthy that the Secretary of State, who has a vested interest in the outcome of the processing of personal data falling within his/her political responsibility, provides the text for any specific data sharing Code of Practice under Digital Economy Act 2017.

This is a conflict of interest; allowing a controller to draft the Code which describes how it processes personal data is like putting Count Dracula in charge of blood donors.

Problem 12: "A Flexible framework to make Ministerial life easy"

The same conflict of interest occurs in the "*Framework for Data Processing by Government*" described in Sections 194(4)&(5) of the DPA2018; this could fetter the ICO when enforcing the DPA2018.

The fettering arises because it is the Secretary of State (and not the ICO) provides the text of this Framework which **must** be considered by the ICO and the Courts when dealing with data protection issues. You can see the problem if the Framework (or Code of Practice) contains provisions that the ICO thinks are improper.

Like Codes of Practice (Problem 11), the text of the Framework could reflect departmental interests for its own personal data processing rather than the appropriate protection for data subjects.

Problem 13: International crisis! Tanks on the lawn

The publishing, via FOI, of 15 year old information relating to legislation which has been repealed (the DPA1998 and Directive 95/46/EC), and where the vast majority of issues subject to dispute have been resolved.

As some blog readers may know, the UK Government has tolerated a defective DPA1998 since 2004 and I have been trying to find out why by the FOI regime. The ICO, in its latest Decision Notice (see references) has again agreed with the European Commission and DCMS that release of this information would seriously prejudice international relations and the current adequacy negotiations.

The DCMS has even told me that if I were to get the request information, a Diplomatic Note would have to be written. It's not quite French tanks parked on the lawns of Buckingham Palace; but it's a small first step in that direction.

Forget the fact that Boris Johnson called the EU a Nazi state, or the diet of disparaging comments from Ministers about the EU that regularly appear in the tabloids; that does not prejudice international relations between the EU and UK.

The real damage and prejudice to international relations is caused if an ageing bald bloke from Barnsley obtained some ancient information relating to repealed legislation.

Sadly, this is not a joke!

Upcoming Data Protection Courses (in New Year)

All courses lead to the relevant BCS qualification:

- **Data Protection Foundation: London, Jan 19-21 (3 days)**
- **Data Protection Upgrade Practitioner: London, Feb 23-24 (2 days)<LAST ONE**
- **Data Protection Practitioner: London, Starts Jan 12 (6 days)**

Full details on www.amberhawk.com of by emailing info@amberhawk.com

References

PM's statement (Statement UIN HCWS86, 20 Feb 2020).

Brexit DP Regulations: *Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) SI 2019/419*

https://www.legislation.gov.uk/uksi/2019/419/contents/made

Gibraltar adequacy: see Schedule 21, paragraph 5(1)(b) of Brexit DP Regulations (above).

ICO Guidance on Confidential Refences: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ex34.

Official explanation for the exam script exemption: *DCMS Document prepared for Adequacy Discussions: "E3 (Schedule 2 Restrictions)"*.

Problem 13: Decision Notice **FS50812647** explains why these details will cause "substantial" prejudice to negotiations with the EU. Details of infraction proceedings See this reference and links at the bottom of the text: https://amberhawk.typepad.com/amberhawk/2019/02/questions-concerning-the-dpa1998-haunt-the-uks-approach-to-gdpr-implementation-and-threatens-adequac.html.