Big Data in the Post-Brexit Era - Where Oh Where Will It Be?

Joseph Dalby SC and Flavia Kenyon, barristers at 36 Commercial, examine the reasons and implications of big data and social media giants moving UK-data overseas.

Google has reported (exclusively by Reuters[1]) that personal data, stored in Ireland, but belonging to UK residents will be moved to the US, supposedly prompted by Brexit. Meanwhile, and it may or may not be connected, Ireland's Data Protection Commission, ('DPC') has released its annual report, which disclosed that it has launched 21 investigations for GDPR violations, including eight involving Facebook. To mark the occasion, the Irish Commissioner, Helen Dixon, gave the clearest signal yet that penalties for an infraction could well be substantial.

Are the two linked? Because in other news it is reported that the amount of time hackers spend inside the networks of compromised organisations before being uncovered has massively declined across Europe -- and GDPR is a key reason for the drop.

---

[1] https://www.reuters.com/article/us-google-privacy-eu-exclusive-idUSKBN20D2M3

First things first, the prospect of big data being removed from the jurisdiction is significant, the full implications of which have yet to be worked out, but potentially leaving tens of millions of Britons' data without a domestic remedy. Presumably Google will procure each data subject's consent to the removal, and there is nothing to stop them from doing so. But data protection in the US is a pale imitation of EU standards that people are getting used to. There is supposedly a privacy shield arrangement in place in relation to EU-data subjects, to replace the safe harbour that was struck out as unlawful by the European Court of Justice.

At the end of the transition period, marking the UK's graduated exit from the EU, the GDPR (and with the privacy shield) will cease being directly applicable in relation to the regulation of personal data of UK residents (*"data subjects"),* except to the extent organised by the **EU (Withdrawal) Agreement 2018**, and replicated through the domestic legislation that was used to ensure effective enforcement of the GDPR in the first place.

Married to this, pursuant to powers under the **EU (Withdrawal) Act 2018,** the Secretary of State passed a new legal instrument: the **Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, ('the 2019 Regulations'),** *"to correct deficiencies in EU-derived data protection legislation as a result of the withdrawal of the United Kingdom from the EU, […]. This will ensure that the legal framework for data protection within the UK continues to function correctly after exit day."*

The data protection regime in Ireland is a matter of Europe-wide concern, because of the amount of big data stored within its jurisdiction, not least from the more populous social media giants, but also the data analytics that they source. Several important judgments have been given by the European Court of Justice, involving Facebook and Google, and have been in cases that originated in the Irish courts, particularly in relation to data that is held within the US safe harbour.

The work of the Irish DPC has increased markedly over the last few years. More than 6,700 data breaches were notified last year, the second highest level of notifications recorded per capita across Europe. This marks a 12 per cent increased compared to 74.9 breaches recorded in for the first eight months of GDPR, when the State was ranked in fourth place per capita across Europe.

The concentration of data within its jurisdiction means that it is at the front line in regulating those companies that store all its data within Ireland. The DPC has not been without criticism both at home and abroad, particularly in relation to its resources to investigate complaints and enforce the law. However it has also attracted criticism for being less than robust with the Irish state in relation to data protection law transgressions whilst relying upon the Government for funding.

Did it, some were speculating, have the grit to impose substantial fines of the order, say, of £183m imposed on British Airways by the Information Commissioner's Office in July 2019, or €50 million imposed by CNIL (France) on Google? Under GDPR, data regulators have the power to fine

companies up to 4 per cent of their global turnover of the previous year or €20 million, whichever is greater, for violating the law. In November the DPC forewarned not to expect any fines in the short term. The largest fine issued in a cross-border context, according to the Data Protection Commission, has been €61,000. Not perhaps surprising therefore that grumbles were heard from Germany about the unacceptable delays and possibly lack of sufficient funding to carry out this frontline mission. In 2020, the budget increased by only €1.6 million to €16.9 million — reportedly less than one third of the funding that the DPC requested from the Irish government.

Confronting the doubts, the Irish DPC remarked to the Irish Independent[2] that under the GDPR, deterrence is a particularly important reason why the fines are included, adding that the $4.5bn fine imposed on Facebook by the US Federal Trade Commission, was 'relevant' in terms of what quantum will create a deterrence. Now this may or may not be code for comparable, but it is an indication that deterrence is a driving factor in assessing the appropriate level of fines and in that regard could not arguably be less than substantial.

Returning to Google, and the recent news about its plans to move its British users' accounts out of the control of EU data protection laws to the US.

---

[2] https://www.independent.ie/business/technology/get-ready-tech-giants-large-fines-may-be-coming-from-dpc-38979824.html

Firstly, one must dispel the idea that Brexit somehow weakens the bite of UK data protection laws, and that somehow UK residents' data is left vulnerable. That is not the case. Substantively, in terms of data protection standards, rights, and remedies of data subjects, the UK data protection regime should preserve and enshrine them unchanged, and with the same force.

On the topic of Jurisdiction, paragraph 2.14 of the explanatory memorandum to the **2019 Regulations** makes clear the territorial scope: *"This instrument maintains the data protection standards that currently exist under the GDPR and the DPA 2018 […] It also maintains the extra-territorial scope of the GDPR, so that controllers or processors based outside the EEA which are processing UK residents' data for the purposes of providing goods and services or monitoring behaviour will continue to be covered by the UK GDPR, and extends this to cover such processing by controllers and processors in the EEA. A number of functions conferred on the European Commission by the GDPR will be transferred to the Secretary of State and/or the Information Commissioner."*

Article 3(1) of the UK GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller/processor in the UK, regardless of whether the processing takes places in the UK or not.

Article 3(2) applies to the relevant processing of personal data of UK data subjects by a controller/processor not established in the UK where the

processing activities are related to either the offering of goods or services to such data subjects in the UK or the monitoring of their behaviour as far as their behaviour takes place within the UK.

It is noteworthy that the UK GDPR specifically preserves the extra-territorial scope of the EU GDPR and offers the same level of protection to all UK data subjects whose data is being controlled/processed by controllers/processors based outside the EEA, and within the EEA.

One important issue triggered by the UK leaving the EU is the issue of international transfer of personal data. According to Art 45 and 46 of the EU GDPR, data processors/controllers may not transfer personal data outside the EEA unless there is *an adequacy decision in* place. The European Commission determines if a particular country/organisation provides an *"adequate"* level of protection for personal data.

The 2019 Regulations amend the UK GDPR and Data Protection Act 2018 ('DPA') so that under Art 45 of the UK GDPR and s 17 A of the DPA, the powers vested in the European Commission in respect of making adequacy decisions are now transferred to the Secretary of State.
Through '*adequacy regulations'*, the Secretary of State has the power to specify that a third country/territory/sector/international organisation ensures an adequate level of protection of personal data of UK subjects.

In Google's case, whatever the motivations behind its decision, the UK GDPR and the 2019 Regulations bite, (Article 3(2)). Google, as a controller and processor of personal information of UK data subjects, is

required to act in accordance with the UK GDPR. Google cannot simply "move" UK users' accounts "out of control" of UK GDPR privacy and data protection laws placing them under US jurisdiction instead.

Furthermore, the Secretary of State through an *"adequacy regulation"* has the power to specify that the US level of data protection of UK data subjects is inadequate. The onus is very much on Google to satisfy the adequacy of data protection.

There is already a useful precedent for bringing mass data breach claims in the UK: ***Lloyd-v-Google [2018] EWHC 2599*** – a privacy class action lawsuit against Google was brought on by four million iPhone users with regards to Google using tracking cookies to override iPhone users' privacy settings in Apple's Safari browser. The landmark decision sets down an important legal principle: a claimant can recover damages for loss of control of their data under section 13 of the Data Protection Act 1998, without having to prove pecuniary loss or distress.

Joseph Dalby SC
Flavia Kenyon, Barrister
36 Commercial **March 2020**