****

**Exiting the European Union and data protection debate briefing 12th of October**

At first glance, the issues of data protection and leaving the European Union are only loosely connected to one another. However, the design, extent and provisions of **the British data protection framework will have profound implications for the nature of EU-UK trade relations post Brexit**. This should therefore be a prominent consideration in the design and implementation of the Data Protection Bill.

Data is an increasingly vital commodity. The UK conducts three quarters of its cross border data exchange with the European Union.[[1]](#footnote-1) **The EU data economy was worth € 272 billion in 2015 and has continued to grow rapidly since.[[2]](#footnote-2)**  The EU has regulated this commodity through the GDPR (General Data Protection Regulation). The GDPR will be legally binding in the UK from May 2018 onwards. This is highly significant to the UK economy, as GDPR:

* Significantly widens the definition of ‘personal data’
* Removes the assumption of consumer consent
* Carries severe fines for companies in case of non-compliance
* Fundamentally alters the way corporations can store and process personal data

The European Union’s data protection framework specifies that ‘third country’ rules will apply, without exception, to any country outside the EU and EEA. This is highly relevant to the data exchange between the UK and the EU because personal data can only be transferred to third countries when an adequate level of protection is guaranteed. Regulatory compatibility and ease of data exchange between the UK and the EU is therefore vital.

An adequate level of data protection can be achieved in **two ways**: The UK could receive an **‘adequacy decision’** from the European Commission post Brexit. Such a decision would clarify that the UK’s data protection framework is equivalent to that of the EU. Alternatively, individual organisations holding and/or processing personal data can seek to make their own data protection arrangements through **Contractual Clauses and Binding Corporate Rules**. However, the legality of such clauses has been **challenged in the recent Schrems II ruling**.

While there are pitfalls and dangers associated with both paths, most experts agree that an **adequacy decision would be the preferable solution**. Elizabeth Denham, the UK information commissioner testified to a House of Lords EU Home Affairs Sub-Committee:

“The best way forward is to achieve an adequacy finding from the EC because it is the most straight-forward arrangement for data flows between the UK and the European Union to continue”.

The biggest objection to this path is **time**. Obtaining an ‘adequacy decision’ is only feasible for third countries. It follows that in order to obtain an adequacy ruling, the UK will have had left the EU already at the time of the ruling, leading to the very real danger of a **‘data protection cliff edge’**.[[3]](#footnote-3) Stewart Room, Head of Data Protection at PricewaterhouseCoopers said on record that obtaining such a decision could take ‘many, many years’.[[4]](#footnote-4) However, countries with more heterogeneous data protection systems than the UK, such as New Zealand and Israel for instance, have obtained favourable adequacy decisions from the European Commission.

**The government** appears to share the view that an adequacy decision would be the best possible solution to ensure the **‘unhindered exchange of data, within an appropriate data protection environment’, that Matt Hancock, Minister of State for Digital and Culture, spoke of.** In the Partnership paper published by the government, it is clearly stated that future data protection cooperation ‘could build on the existing adequacy model’.[[5]](#footnote-5)

To achieve this stated objective, ensuring the continued **alignment of the UK’s data protection framework with the EU’s will be key**. This should therefore be the foremost consideration in any discussion of the provisions of the Data Protection Bill. Deviating too much from the provisions of the GDPR could risk a successful outcome in the European Commission’s adequacy decision.

* A Data protection Bill containing key provisions of GDPR would sacrifice some benefits of a more bespoke law, but probably reduce the time needed by the EU Commission to reach an adequacy decision

Given the close alignment of the UK and EU data protection frameworks under this scenario, the government should prioritise ICO involvement in the formulation of future EU data protection provisions.

**🡪This would alleviate risk of the UK becoming a passive rule taker without a say in the formulation of those rules.**

1. HOL 3rd report of Session 2017-19 ‘Brexit: the EU data protection package’ [↑](#footnote-ref-1)
2. Future Partnership Paper, ‘The Exchange and protection of personal data’ [↑](#footnote-ref-2)
3. https://panopticonblog.com/2017/08/24/brexit-and-data-protection/ [↑](#footnote-ref-3)
4. House of Commons Library, Briefing Paper Number 7838, 27th July 2017 [↑](#footnote-ref-4)
5. Future Partnership Paper, ‘The Exchange and protection of personal data’ [↑](#footnote-ref-5)