DATA PROTECTION AND DIGITAL INFORMATION BILL

International transfers and data adequacy

Summary: The Data Protection and Digital Information Bill (the 'Bill') introduces a lower standard for transfers of data out of the UK than from out of the EU. This presages divergence between the list of countries granted 'adequacy' by the UK and EU respectively, which will necessitate complex geofencing and monitoring of data coming from the EU to the UK. The extensive reliance on secondary legislation in the Bill also introduces uncertainty about how the UK's regime will develop.

As well as placing burdens on businesses, these changes may well leave a question mark over the long-term future of the EU's adequacy decision regarding the UK, disincentivising investment in the UK and causing difficulties for UK businesses.

Lower standards for international transfers of personal data

1. s.21 and Schedule 5 of the Bill introduce a new UK-specific regime under which personal data may be transferred to third countries. The main changes are:

   i. The Secretary of State is empowered under new Article 45A to issue regulations ('approval regulations') that permit the transfer of personal data from the UK internationally. These approval regulations function in a similar way to adequacy decisions under the EU GDPR. They can be issued where the 'data protection test' under new Article 45B is met. This data protection test is analogous to the requirement in Article 45(1) EU GDPR that a country awarded an adequacy decision 'ensures an adequate level of protection' – which has been interpreted as meaning that the standard of data protection must be 'essentially equivalent[1]. The data protection test in Article 45B UK GDPR, however, is that the standard of data protection in the relevant third country is 'not materially lower' than that in the UK. It is not clear from the wording alone what is intended by this change from "essentially equivalent" to "not materially lower". Whilst the Government's consultation response states

[1] Case C-362/14, *Schrems II*

that the new regime will 'retain the same broad standard that a country needs to meet in order to be found adequate', it is difficult to see why the wording of the test would be changed unless with the intention is to allow transfers to countries with lower standards of protection than currently qualify for adequacy under the EU GDPR.

ii. The data protection test in Article 45B differs from the adequacy test under the current GDPR regime in a number of respects, with the effect of giving the Secretary of State greater latitude in making approval regulations:

   a. It does not require consideration of whether there is an independent and effective supervisory authority in the third country;

   b. It replaces the need for 'administrative and judicial redress' with 'judicial or non-judicial redress' (a key issue in the Privacy Shield dispute).

   c. it permits consideration of the 'constitution and traditions' of the third country, though it is not clear from the Bill – or the Government's consultation response – how such factors affect consideration of the data protection test.

iii. The Secretary of State may consider 'the desirability of facilitating transfers of personal data to and from the United Kingdom' (Article 45A(3)) in making regulations under Article 45A, which again appears designed to increase the range of countries in respect of which approval regulations may be made.

2. The 'data protection test' is used to assess the lawfulness of any standard data protection clauses promulgated by the Secretary of State under new Article 47A (effectively UK-issued standard contractual clauses).

3. The overall impact is that it is likely that controllers in the UK will have greater freedom to transfer personal data to a wider range of third countries than under the current regime (and by extension than controllers subject to the EU GDPR)[2].

[2] Indeed this is consistent with stated UK government policy - https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare - and with the way these changes are described in the Government's consultation response.

Depending on how the UK's adequacy and standard clauses regime develops, this could dilute the protection of UK data subjects' personal data.

EU's adequacy decision in respect of the UK

4. This change also implies the potential for personal data to be transferred from the EU to the UK (under the UK's adequacy decision from the European Commission), then onward from the UK to a third country not benefiting from an EU adequacy decision; this would undermine the EU GDPR.

5. The EU has sought to address a similar issue when granting its adequacy decision to Japan. As part of that decision, supplementary rules[3] provide for additional safeguards binding on Japanese companies importing data from the EU and enforceable by the Personal Information Protection Commission and Japanese courts. The supplementary rules include restrictions on onward transfers of data. In sum, if a Japanese business operator is transferring relevant EU personal data to a third country, informed consent of the EU data subjects is required unless the third party is in a country which is recognised to guarantee equivalent protections, or measures have been implemented (such as contract or other binding agreement) providing equivalent protections. Similar provisions apply to the adequacy decision for The Republic of Korea. That is, data transferred from the EU to Japan and Korea under the adequacy decisions must be both technically and legally 'geofenced' to protect it from onward international transfer.

6. It is possible that the UK's adequacy determination from the EU would be modified by similar supplementary rules (indeed this seems likely given the UK Government's stated intention to make regulations allowing transfers of personal data from the UK to a range of countries not benefiting from an EU adequacy decision). This would require geofencing of data transferred to the UK from the EU – a significant burden for UK controllers. Adherence to the supplementary rules would require ongoing monitoring by the EU, potentially leaving a question

[3] https://ec.europa.eu/info/sites/default/files/annex_i_supplementary_rules_en.pdf

mark over the UK's adequacy decision, which could be challenged before the Court of Justice of the European Union (CJEU).

Consider for example US-headquartered controller which might process in the UK both data originating in the UK, and data originating in the EU. If the UK makes regulations under Article 45A UK GDPR permitting transfers to the US (and assuming the US continues *not* to benefit from an adequacy decision from the EU), that controller could transfer the UK-originating data to the US, but would need to be able to demonstrate that any EU-originating data was protected from being transferred to the US. This may be very difficult to do in practice. If it were shown that EU-originating data was generally at risk of being transferred to the UK and then on to the US, this would be grounds for bringing a challenge against the European Commission seeking to invalidate the UK's adequacy decision.

7. This issue could only be fully addressed by aligning the UK's own international transfers regime with adequacy decisions issued by the Commission, which is very unlikely. Short of this, an improvement would be to more tightly define the data protection test, to reduce the level of divergence between the lists of EU-adequate and UK-adequate jurisdictions.

Independence of the Information Commission

8. In granting an adequacy decision under Article 45 EU GDPR, the Commission must consider (inter alia) *"the existence and effective functioning of one or more **independent** supervisory authorities."* (emphasis added).

9. The Bill reduces the independence of the UK's supervisory authority – the ICO (to be renamed the Information Commission) – to a degree, which may undermine the UK's adequacy decision.

10. S.28 of the Bill introduces §120E-H into the DPA which, in sum, allow the Secretary of State to designate "strategic priorities" to which the Information Commissioner must 'have regard' (though these are subordinate to the

Information Commissioner's principal objectives – s.120A). Whilst this is a significant change, s.120F(2) clarifies that the duty to have regard to the priorities does not apply when the Commissioner is carrying out specific investigations. It is doubtful therefore that this *alone* compromises the independence of the regulator to the extent that the test under Article 45 EU GDPR is no longer met.

Instability in the level of protection of personal data

11. The Bill makes extensive provision throughout for important provisions to be amended and varied by the Secretary of State through the introduction of statutory instruments according to various parliamentary procedures. These include adding interests in processing which may automatically qualify as a lawful basis without any need to balance them against data subjects' interests, among other matters which are fundamental to the protection of personal data.

12. Predicting the impact of this on the UK's adequacy determination requires a distinction between (i) the status and impact of the Bill itself on the day it becomes law, and (ii) the potential that it introduces for longer-term change to the UK's data protection regime.

Immediate impact

13. By leaving important matters of data protection subject to change through secondary legislation (i.e., without further primary legislation) and therefore full parliamentary scrutiny, it could be argued that the Bill creates a data protection regime that is too ill-defined and/or liable to change over time for the UK's adequacy decision to be meaningful. That is, the European Commission would not be able to assess whether or not standards of data protection in the UK meet the relevant test in the EU GDPR for data adequacy.

14. It is unclear however, the extent to which the Commission is likely to inquire into the specifics of how secondary legislation is made in the UK, or whether it would be willing to effectively imply that the use of statutory instruments is arbitrary or not consistent with the rule of law. Article 45 EU GDPR also already provides for the protection of personal data in countries with adequacy to be monitored, which would allow the Commission to respond to any future fundamental reductions in

data protection in the UK via statutory instrument. It is unlikely that the mere presence in the Bill of the ability to create secondary legislation would prevent the Commission from renewing the UK's adequacy determination, once it becomes law.

Longer-term impact

15. Over time, secondary legislation may lead to significant changes to the UK's data protection regime. There is likely to be anxious scrutiny of the way the UK's data protection regime is developing from the European Commission. Major changes could well prompt the Commission to reconsider whether the UK continues to meet the test in Article 45 GDPR.

16. Data adequacy is not only a political matter for the European Commission. It will face scrutiny before courts and data protection authorities. Individuals may bring cases before the CJEU (as has happened in relation to adequacy for the US) where they consider secondary legislation has changed the UK's regime to such an extent that an adequacy decision from the European Commission should no longer stand.

17. Thus while the role of secondary legislation in the Bill does not necessarily imperil the UK's adequacy on the day it becomes law, it leaves a real question mark over the long-term future of the UK's adequacy decision, depending on how that secondary legislation is used to change the data protection regime. This in turn will undermine business confidence and investment.

18. To reduce this risk, the Government could limit the use of secondary legislation to less consequential aspects of the data protection regime.