IRSG Data workstream

IMPACT OF BREXIT ON PERSONAL DATA TRANSFERS

The International Regulatory Strategy Group (IRSG) is a practitioner-led body comprising leading UK-based representatives from the financial and professional services industry. It is an advisory body both to the City of London Corporation, and to TheCityUK. The Data workstream includes representatives from financial services firms, trade associations, the legal profession and data providers.

Summary

It is the view of the IRSG Data workstream that the most legally sound and stable option of ensuring the continued ability to transfer personal data between the UK and the EU27/EEA and international destinations, is to secure mutual adequacy decisions between the EU and UK.

It is important to avoid any gap between the UK's withdrawal from the EU and adequacy, so potentially transitional arrangements also need to be developed.

A key step towards ensuring this will be a consistent implementation of the General Data Protection Regulation (GDPR) by the UK, coupled with an ongoing alignment with its provisions post Brexit.

The proposed approach put forward by HMG in the Future Partnership Paper provides the ambition but not the certainty and detail necessary for business to develop their Brexit plans in the context of personal data.

Background

The UK is currently undertaking the process of implementing the GDPR, which has a deadline of May 2018. Its requirements are more rigorous than the existing Data Protection Act (1998). Businesses processing and/or monitoring EU citizens' personal data will be subject to the GDPR, the new UK data protection law and ICO regulation will ensure this will continue post Brexit.

We understand that the European Union (Withdrawal) Bill will incorporate the complete body of EU law into UK law at the point of departure from the EU[1]. However, it is anticipated that at that point the UK will become a third country, and appropriate grounds for permitted data-transfer will need to be established. To ensure that businesses can continue to operate on a cross-border basis, an arrangement is therefore urgently required to ensure the ongoing free flow of personal data post Brexit.

[1] See the IRSG Report 'The Great Repeal Bill': Domesticating EU Law', published 27 June 2017

The following options are considered below:

1. Adequacy decision

We believe that an Adequacy decision for the UK is the most legally sound and stable option and corresponds to the approach set out by the UK Information Commissioner on 8 March *(foot-note: House of Lords Home Affairs Sub-Committee).* True, reliance on a Commission decision will raise the vexed question of whether mutual recognition would be a preferable approach and whether the UK should be a "rule-taker", rather than a "rule-maker" in this area.[2] The IRSG believes however that a data-adequacy decision currently offers the most certain option of providing an overarching framework for future personal data transfers.

This needs to be coupled with an adequacy decision by the UK in respect of the EU, in order to ensure that transfers can also continue from the UK to the EU.

In addition, the UK should continue to accept and enable companies to rely on Binding Corporate Rules that have been approved prior to departure. Beyond departure, a mutual recognition procedure should be established to approve in an expeditious manner, new Binding Corporate Rules that have been approved by the ICO or vice versa in the EU under the regular GDPR procedures.

i. What needs to be done?

As the GDPR will come into force prior to the UK's departure from the EU, the UK should seek to implement it in such a way as to ensure that the UK is technically compliant at the point of departure from the EU.

Beyond departure from the EU, the UK should ensure that its approach to GDPR does not diverge in a way that could prevent an adequacy finding from being given or maintained. Our current understanding is that there is no legal reason why the UK cannot apply for adequacy before it becomes a third-country, and therefore the UK Government should request that the Commission begin the preparatory work now to ensure a decision is achieved prior to Brexit, which can be activated on Brexit. This is not just in the interests of the UK, but given the significant flows of personal data in both directions between the UK and the EU27, and beyond the EU as well, it is in the broader interests of international trade to limit disruption to an absolute minimum. It is beneficial for all countries to have a common framework and standards and to avoid fragmentation.

Finally, the EU will also benefit from maintaining the UK within a GDPR-based data protection framework. Should the UK, a jurisdiction which has implemented GDPR, not be considered adequate by the European Commission, it will send a discouraging signal to other third-countries considering

[2] This has been fully discussed in the IRSG Reports "The EU's Third Country Regimes and Alternatives to Passporting", published on 23 January 2017, and "Mutual recognition – a basis for Market Access after Brexit", published on 11 April 2017.

applying for adequacy, or to third-countries with existing adequacy decisions which will soon be up for review. This may result in further fragmentation of international frameworks and standards.

A further useful step would be to seek some form of UK membership (such as observer status) for the ICO on the European Data Protection Board (EDPB) post Brexit. This would be mutually beneficial, with the ICO contributing considerable expertise and resource to the EDPB.

ii. Transition: the importance of avoiding a 'gap' or 'cliff edge'

If any future adequacy process is not completed prior to the UK's departure, as is likely to be the case (based on what is usually regarded as a two year negotiation period), it will be essential to put in place an appropriate transitional period to ensure the continuing flows of personal data and to avoid a "cliff edge" scenario. This is linked to the broader set of transitional arrangements, highlighted by the Prime Minister in her recent speech in Florence, which will be required in relation to the overall interim UK/EU27 relationship, and form part of the current negotiations.

iii. What happens if an adequacy decision (or transition) is not in place on Day 1 of Brexit?

If there is no transition arrangement, the following arrangements could technically be used. These were considered by the workstream as permanent alternatives to adequacy, but were discounted as clearly inferior to an adequacy decision for the following reasons:

a. **Consent**	This can be withdrawn or withheld at any time making it unreliable for important activities like financial crime prevention
b. **Binding Corporate Rules**	These are valid for intercompany personal data transfers only. The approval process can be slow and if there is a significant increase in applications it could have resourcing implications for the ICO. They are also only available to companies with a presence in an EU Member State. Further, this process is time consuming and complex to design and secure and requires continuous updating. They are not a feasible solution for smaller firms who do not have a group level presence.
c. **Model contracts**	These are more flexible but do not provide legal certainty, as they are currently subject to a legal challenge[3]. In addition, the identification and renegotiation of relevant contracts can be time consuming and complex, and they are not well suited to transfers in a group using a branch structure.

[3] 2016/4809P

d. Legitimate interests derogation	There are limitations on the size and frequency of transfers, coupled with a requirement to notify the Data Protection Authority and the data subject, which makes this unworkable for most arrangements or transfers.

iv. UK agreements with non-EU/EEA regimes

As the GDPR will no longer have direct effect beyond Brexit, the UK will no longer be a party to the EU arrangements that have been agreed with "adequate" third countries, and other agreements such as the EU/US Privacy Shield. It will therefore need to develop its own framework for cross border personal data transfers through the creation of bilateral relationships. In doing so, it will need to consider if it should adopt the adequacy decisions that have already been taken by the European Commission (which may themselves need revision to take into account the more stringent provisions of the GDPR and new/pending adequacy decisions covering jurisdictions such as South Korea and Japan). Two important policy considerations will therefore be (1) whether the UK should, as a matter of practice, adhere to all data-adequacy decisions reached by the EU, and (2) the implications for the EU data-adequacy decision in relation to the UK, if the UK sought agreements with countries not deemed data-adequate by the EU and/or agreements with lower levels of protection.

v. The dangers of not being granted adequacy

Without adequacy decisions between the UK and EU, alternative but less attractive and less practical options will be required to ensure continuing data flows (see section iii). This could result in a significant increase in compliance burdens for business in the UK and the EEA. There will also be increased costs particularly in relation to putting new measures in place and a period of legal risk and uncertainty until this is completed. There will also be a degree of uncertainty as to the legal efficacy regarding alternative options due to legal challenges currently in the courts *(see option c. Model contracts above).* This situation will create significant challenges for the growth and development of the digital economy, creating uncertainty for electronic personal data flows which are now an absolute necessity in the on-line world, and for businesses offering services beyond their immediate geographical boundaries.

2. <u>Separate bilateral "UK/EU Privacy Shield" arrangement</u>

We do not believe a Safe Harbour/Privacy Shield mechanism is a viable alternative to an adequacy decision. It would likely be sector specific, and in parallel with the GDPR, which will be implemented in the UK on a cross-sectoral basis. The two systems would therefore differ in coverage, leaving it unclear how "gaps" would be addressed. It would also potentially be open to legal challenge. The European Commission has publicly stated that the 'Privacy Shield model' is not one that it would like to see replicated between the EU and other jurisdictions, and it is already the subject of legal challenge.

3. Arrangements on personal data-transfer within a UK-EU Free Trade Agreement (FTA)

The government has said that it will pursue "a new strategic partnership with the EU, including an ambitious and comprehensive Free Trade Agreement"[4]. Such an FTA would be of unprecedented scope and depth, and could potentially include provisions on protection of personal data. Negotiations for such an FTA have not yet started, and the inclusion of data protection provisions would require the agreement of both sides. It is not clear whether this would be forthcoming from the EU: historically, EU FTAs with third countries have tended to avoid extensive provisions on data-privacy (on which the EU has tended to prefer its own data-adequacy decision-taking process). What is more, terms and conditions for the inclusion of provisions on data in EU FTAs are currently the subject of unresolved debate within the EU institutions. For these reasons, an EU agreement to include data protection provisions within an FTA (e.g. on a mutual recognition basis) may not be readily forthcoming. All this suggests that, while the FTA option should not be excluded, an approach based on data adequacy looks likely, at this juncture, to prove the more practicable.

4. HMG Future Partnership Paper on the exchange and protection of personal data

HMG has recently published a Future Partnership Paper which sets out the proposals for the UK and the EU to "agree a UK-EU model for exchanging and protecting personal data". This could build on the existing adequacy model. In advance of this the paper also proposes that the EU and the UK agree early in the process to "mutually recognise each other's data protection frameworks as a basis for the continued free flows of data between the EU (and other EU adequate countries) and UK from the point of exit until such time as new and more permanent arrangements come into force".

If such mutual recognition could be achieved by March 2019, that would be most welcome, but we do not believe that the approach as suggested provides sufficient detail and certainty at this stage to enable businesses to plan for a smooth Brexit transition. The proposal runs the risk of getting caught in the political process surrounding Brexit, which we view with extreme concern, as the outcome will likely be reached too late to provide business with sufficient time to prepare fully.

5. Conclusion

The key requirements to ensure the continued cross-border transfer of personal data:

- **UK to undertake full implementation of the GDPR by May 2018**
- **Assessment and removal by HMG of likely obstacles to the UK achieving an adequacy decision**

[4] White Paper

- **HMG to request the European Commission to begin pre-departure preparations for an adequacy decision**
- **HMG to seek an appropriate set of transitional measures to avoid a cliff-edge scenario and seek 'in principle' agreement as soon as possible in order to provide business certainty**
- **UK to continue to maintain high data protection standards post Brexit to support an adequacy decision remaining in situ**

January 2018