Data protection – or protectionism by the back door?

July 2017

Current trends in data protection are creating pressures against transferring data out of an individual's home jurisdiction and, if allowed to continue, these trends could carve-up markets and erect barriers to free trade.

This briefing was first published in Privacy Laws & Business UK Report, Issue 91.

Current challenges to the regime for international data transfers coincide with increasingly nationalist and protectionist rhetoric in western countries. We believe that it is essential that the courts strike an appropriate balance between the imperatives of protecting data and facilitating free trade, and that it would be regrettable if data protection legislation were used as a means to introduce protectionism by the back door.

Erecting barriers to free trade may not have been the European Union's intention behind implementing and strengthening its data protection regime through the Data Protection Directive and, from May 2018, the General Data Protection Regulation. There is a concern, however, that recent developments could have exactly that effect, introducing protectionism under the cloak of data protection.

The EU's citizen-focused data protection framework currently finds itself locked in a conflict with the policy imperative of boosting cross-border trade. This imperative sustains that the more easily data can flow out of a home country, the more easily foreign corporations can sell their products and services to customers in that home country, resulting in increased choice and competition, better products and services, and lower prices for consumers.

The EU legislative framework seeks to protect data in a manner which prejudices neither privacy rights nor freedom of trade. It offers various international data transfer methods to allow data to be legitimately off-shored whilst protecting citizens' rights.

Following the Snowden revelations, privacy activists won an important victory when the CJEU invalidated the US-EU Safe Harbour in *Schrems* (C-362/14). Currently, privacy activists are challenging the validity of Standard Contractual Clauses and the US-EU Privacy Shield in the courts. The risk that one or more of these challenges succeeds cannot be disregarded.

Direction of travel: localisation of data

Alongside such challenges, there is an increasing public perception that our data simply is not safe overseas, fostered by continuing and prominent media coverage of snooping revelations (including by WikiLeaks regarding the CIA and MI5 in 2017) and data security breaches affecting millions (including hacking of e-mail accounts, bank account details and health records). Despite government agencies of EU countries having been implicated in snooping and EU companies having suffered breaches, it tends to be non-EU countries that are seen as unsafe destinations for our data.

The combined effect of these challenges and the perception that our data is safer at home is to dissuade some market participants from exporting

data. Exporters come under pressure to set up separate data centres in Europe (as Microsoft has done), and either pass on the costs of doing so to consumers or reduce the range of products and services that they sell in Europe.

Legislators in some countries, including Russia, South Korea and Vietnam, have gone a step further by enacting "data localisation" laws requiring wider categories of data to be stored within national borders. EU countries are not immune to this temptation: some government bodies, for example in Germany, require contractors not to store data outside the country as a condition of appointment. Indeed, the European Commission estimates that removing existing data localisation measures in the EU (to develop a data economy and a Digital Single Market) would lead to GDP gains of up to €8bn per year. However, it warns that "further barriers are likely to emerge from numerous administrative rules and practices and the trend, both globally (+160% since 2006) and in Europe (+100% since 2006), is towards more data localisation".

With local laws and regulations forefront in their minds, businesses regularly ask us to advise where their data should be stored. Overall, the uncertainty caused by challenges to transfer methods means that businesses will incur greater costs, both in transacting business internationally and in analysing and anticipating future developments. Such costs may make their products and services less attractive or may simply act as *de facto* barriers to entry.

What does this mean for free trade?

The current direction of travel is not positive for free trade. Restricting data flows restricts free trade, and carves up markets because it is harder to export to markets which restrict data flows.

These developments come at a time when the credibility of free trade is itself under threat. President Trump's "America first" rhetoric resonated with voters concerned that globalisation causes job losses and that free trade deals such as the North American Free Trade Agreement (NAFTA) have harmed US citizens. The G20 has dropped its pledge to fight "all forms" of protectionism. Ironically, it is the Chinese president who has stepped up to defend free trade. Now more than ever, it is important for the UK and other major economies to defend the benefits of free trade and to promote free movement of the data which supports it.

The UK finds itself at a crossroads, having served notice of its intention to withdraw from the world's largest free trade zone - the EU Single Market - whilst marketing itself as a "beacon of global free trade" after Brexit. The UK government needs trade deals with as many countries outside the EU as possible. It is likely that the UK government will want to facilitate transfers of UK citizens' personal data outside the UK as part of any deal, as it recognises that free movement of data is essential for growth (for example in fintech, in which the UK is particularly keen to establish itself as a world leader). The UK also needs a trade deal with the EU and, critically, a framework to ensure continuity of data flows from the EU to the UK. The Brexit White Paper states: "As we leave the EU, we will seek to maintain the stability of data transfer between EU member states and the UK".

However, the UK could soon find itself in a compromising position. If the UK's post-Brexit approach to international transfers is more relaxed than that of the EU, the European Commission might refuse to grant an adequacy decision for the UK's post-Brexit data protection regime: EU politicians may not be willing to risk adverse media reports that their citizens' data, having been transferred to the UK, was then transferred on to another third country under a relaxed UK data protection regime. In the absence of an adequacy decision, some UK businesses exporting to the EU may be pressured into localising data within the EU, for example by establishing new EU subsidiaries, which would increase compliance burdens and costs for UK exporters. Data protection will play an important

role in determining the nature, and height, of barriers to entry for UK business to the EU market after Brexit, and it remains to be seen whether the UK will be able successfully to persuade its European partners to maintain a balanced data protection regime after the UK ceases to participate in EU policymaking.

In practice: how to approach international transfers in these uncertain times

- Continue to use established international data transfer methods: EU Commission adequacy findings, Standard Contractual Clauses and Binding Corporate Rules. Despite current challenge in the courts, they remain valid for the time being and policymakers are aware of their importance.
- Ensure that Standard Contractual Clauses are used specifically and appropriately, compliance is monitored and any breaches are enforced. Consider carrying out audits on transferees' data handling. The current methods for international transfers are more likely to succumb to challenge if they are not seen to be providing adequate protection for data subjects in practice.
- Implement internal procedures to monitor current developments and react to any changes to the permitted methods for international data transfers. Obtaining institutional buy-in and resources from your organisation's management for this monitoring process is essential given the possibility that changes could occur to the international transfer regime which require amendments to contracts and existing data transfer practices.

Need for a balanced approach

In our opinion, the trend towards greater data localisation and the increasing threats to existing international transfer methods are regrettable. It is, of course, important that citizens' privacy rights are respected and that appropriate remedies are available where those rights are violated as required under the EU Charter of Fundamental Rights. However, it should be possible to facilitate trade whilst also protecting data in a stable, clear and proportionate data protection regime.

There are some encouraging signs. Angela Merkel, the German chancellor, has argued in November 2016 that EU countries should not be too restrictive in their application of data protection laws, recognising the impact this could have on innovation and trade: "Courts will have to be careful not to be too strict if that means limiting opportunities". [1]

At the same time, it is important to address citizens' cyber security concerns. High-profile data security breaches have occurred in our "home" countries in the EU, and these breaches undoubtedly contribute to a general hostility towards international data transfers. In our view,

1 www.theregister.co.uk/2016/11/22/merkel_data_protection_big_data/

strengthening international cyber security practices, together with effective monitoring and periodic reviews of the existing methods for international data transfers, will help to build greater trust in international transfers. Incentivising businesses to improve cyber security, as the UK intends to do following its Cyber Security Regulation and Incentives Review, could provide assurance without the need for further restrictions on data.

Legislators and governments must also enact sensible national security legislation that appropriately respects the rights of individuals. Fear of government 'snooping' underlies the current challenges to international data transfers, and governments must recognise that wide-ranging encroachment on privacy in the name of national security can affect free trade.

The role of the courts

After a five week trial in Dublin, the Irish High Court is considering whether to refer Maximilian Schrems's challenge against use of Standard Contractual Clauses for transfers to the US to the CJEU. If a referral is made, judgment from the CJEU may emerge within a year. Preliminary rulings are expected from the CJEU later this year on the challenges being brought by Digital Rights Ireland and Quadrature du Net against the US-EU Privacy Shield.

The courts have a vital role to play in maintaining a balanced approach to data protection and free trade. It would be unfortunate if the CJEU were to decide any of these cases on the basis of technicalities, as they arguably did with the US-EU Safe Harbour. We hope that the CJEU will see these challenges in their wider context and appreciate their wider implications for free trade if they were to succeed.

Ultimately, free trade is a reciprocal issue because trade is bilateral and multilateral: if our courts and legislators erect barriers to entry, those of our trading partners are likely to follow suit. This would mean that the admirable goals of data protection will be turned into the own goal of introducing protectionism by the back door. If that were to happen, no one would benefit.

This article was written by Rob Sumroy and Andrew Chaplin. Slaughter and May advises on all aspects of data protection and privacy, including GDPR compliance audits. If you would like further information, please contact Rob, Andrew or your usual Slaughter and May advisor. Further publications are available on our website.

Rob Sumroy
T +44 (0)207 090 4032
E rob.sumroy@slaughterandmay.com

Andrew Chaplin
T +44 (0)20 7090 4285
E andrew.chaplin@slaughterandmay.com

Dated July 2017