Adequacy in data exchange: safeguarding flows

With Brexit still high on the world stage and the European agenda, how does the EU determine if a non-EU country, which the UK is on course to become, has an adequate level of data protection? What will really apply if and after the UK leaves and becomes a non-member state – waiver, inclusion, shield or reform?

Currently, personal data can flow freely throughout the European Union's member states as the intra-EU data transfer arrangements organisations put in place, are subject to EU data protection laws. That is set to change with the UK on course to end its EU membership.

EU data protection law places restrictions on the transfer of personal data outside the European Economic Area (EEA). Businesses are prohibited from transferring personal data to non-EEA countries unless they have in place one of a number of safeguards to ensure EU data is adequately protected when processed in those 'third' countries.

One mechanism which has helped to facilitate the free flow of personal data between organizations in the EU and non-EEA jurisdictions is the adequacy framework. That provides the European Commission with powers to designate non-EEA territories as having data protection standards in place that are essentially equivalent to those provided for in the EU. To-date, the Commission has issued adequacy decisions for 12 territories, including the US, Canada, Switzerland and New Zealand, and it is in the process of adding Japan and South Korea to that list.

In this regard, the European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection, whether by its domestic legislation or of the international commitments it has entered into.

Adequacy decisions

The adoption of an adequacy decision involves:

- a proposal from the European Commission
- an opinion of the European Data Protection Board
- an approval from representatives of EU countries
- the adoption of the decision by European Commissioners

At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation.

The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

Brexit and data protection

Following the UK Government and the European Commission's announcement that the UK and EU27 countries had reached a draft agreement on the terms of the UK's withdrawal from the EU, part of the agreement included an outline of the political declaration on the future EU-UK relationship with regard to data protetion.

According to this declaration, the Commission will assess UK data protection standards on the basis of the EU's 'adequacy framework' with a view to adopting an 'ad-

UK PM Theresa May and European Commission President, Jean-Claude Juncker

equacy' decision 'by the end of 2020'. Over the same period, the UK will 'take steps to ensure comparable facilitation of personal data flows to the Union', it said.

While the political declaration indicates that a mutual EU-UK 'adequacy' arrangement could facilitate the flow of personal data between the EU and UK after 2020, the draft withdrawal agreement outlines what protections should apply to the UK's processing data about data subjects outside of the UK prior to the end of the Brexit transition period and after that period in circumstances where a future adequacy arrangement is not in place.

Cyber security

According to media giant, Forbes, set against this backdrop of Brexit political uncertainty, is a cybersecurity industry increasingly worried about the post-Brexit threatscape. According to its own research, Forbes says whether the UK crashes out of the EU with or without a Brexit deal, the impact upon cybersecurity is likely to be considerable and immediate for business and industry. Some industry experts say opinion is divided into three main areas of cybersecurity concern: employment, regulatory compliance and information sharing.

International transfers

According to further reports, enforcement of GDPR matters will change under any withdrawal agreement. The Information Commissioner' Office (ICO) will no longer be part of the European Data Protection Board, and will no longer be able to act as a lead

Michel Barnier, Chief European Negotiator for the UK exiting the EU

European Commissioner for Digital Single Market, Andrus Ansip

authority in cross-border processing issues affecting more than one EU country. Businesses that process personal data in the UK and in EU countries may have to deal with the ICO for the UK processing activities and designate a 'main establishment' in an EU country for their EU processing activities.

In the wider world, looking west to data transfer between Europe to the United States, frameworks seem to be in place but reforms are constantly on the table.

In 2016 the EU-US Privacy Shield, a renewed framework for transatlantic data flows, replaced the EU-US Safe Harbor arrangement. The EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce, subject to privacy safeguards and commitments. The Swiss-US shield framework was approved by the Swiss Government in early 2017, comply ing with Swiss requirements.

by Victor March

EU and US shield

At the time of its implementation, approval of the the Privacy Shield preserved a key legal mechanism for EU-US data flows, according to the Future of Privacy Forum (FPF). Continuing challenges were also mooted - surveillance reform needs continue on both sides of the Atlantic - but the Privacy Shield is seen as a much needed certainty for American companies that rely on the EU-US framework to pay and manage their EU-based employees, as well as for the 150 plus EU companies that use the framework to transfer data to their own US subsidiaries.

The Safe Harbor agreement ceased amid concerns regarding US government surveillance programs. The Privacy Shield approval was also implemented in the wake of surveillance reforms and additional commitments by the US government. The FPF detailed more than two dozen significant reforms to US surveillance law and practice since 2013. A previous study revealed that Safe Harbor included 152 companies who are headquartered or co-headquartered in European countries, which span a wide range of industries and countries.

The 152 companies include some of Europe's largest and most innovative employers - many from the world of advanced digital information and ID, doing business across a wide range of industries and countries. According to its raison d'etre, EU-headquartered firms and major EU offices of global firms depend on the Privacy Shield program so that their related US entities can effectively exchange data for research, to improve products, to pay employees and to serve customers. FPF also found that more than 3,700 companies have signed up for Privacy Shield – a nearly 70 percent increase from 2017.

Meanwhile, the European Commission recently published its second annual review of the EU-US Privacy Shield, finding that the US continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the US. This is good news for business, supporting transatlantic trade and ensuring meaningful privacy safeguards for consumers. It is also good news for EU employees and companies, many of whom rely on the agreement to retain and pay staff. The Commission's review highlighted a key next step to support the Privacy Shield arrangement – urging the U.S. government to appoint a permanent Ombudsperson by the end of February 2019.