Reviewing data transfers through the lens of transparency

Hugh McCarthy, Associate with Arthur Cox, gives an overview of recent data transfer developments and explains why data controllers need to understand the evolving data transfer landscape in order to meet GDPR transparency requirements

The international data transfer landscape has changed considerably in the two years since the Court of Justice of the European Union ('CJEU') struck down the EU-US Safe Harbor regime, in the case now known as 'Schrems I'.

As a consequence of Schrems I, Safe Harbor has been replaced by the Privacy Shield, which is itself subject to a pending legal challenge before the General Court of the CJEU, and in a sequel case known as Schrems II, the Irish High Court has recently decided to send a preliminary reference to the CJEU concerning the validity of standard contractual clauses. Simultaneously, the ongoing Brexit negotiations have cast doubt on the status of data transfers to the UK post-March 2019.

While it may appear that data controllers can safely observe these developments from afar, the General Data Protection Regulation ('GDPR') will require otherwise from May 2018. As well as obliging data controllers to comply with new rules on data transfers, the GDPR will also require organisations to both understand and record their data transfer practices and to inform individuals about transfers of their personal data to so-called 'third countries' (i.e. those outside the EU).

Transparency, record-keeping and data transfers

A recent review conducted by the Global Privacy Enforcement Network, and led by the UK's Information Commissioner's Office, found that details about the international transfer of data provided on a range of website and app privacy notices was 'often unclear and vague'. This approach will fall short of the GDPR transparency requirements. Articles 13 and 14 of the GDPR impose specific obligations on controllers to make clear to data subjects:

- if they intend to transfer the data subject's personal data to a third country;
- whether such third country has the benefit of an adequacy decision from the European Commission (see below); and if not;
- in the case of data transfers based on Articles 46, 47 or 49 of the GDPR (see below), provide details of what 'appropriate or suitable safeguards' are in place (and details of where a copy of the safeguards can be obtained).

This information must be provided either at the point of data collection (where data are collected directly from data subjects) or within one month (where the data are obtained from a third party).

Echoing Articles 13 and 14, controllers are required by Article 30 of the GDPR to maintain certain records concerning their data processing activities. These records must include, in particular, the details of any data transfers to third countries — identifying the destination country — and in the case of data transfers based on the second paragraph of Article 49, documentation of the suitable safeguards put in place.

Transparency and record-keeping obligations aside, controllers must also consider Article 5(2) of the GDPR. Article 5(2) provides that controllers are not only responsible for compliance with the new rules, but also for being able to demonstrate compliance – a further reason to keep written records of all data transfers. To meet these transparency, record-keeping and compliance obligations, controllers need to understand the ever-evolving data transfer landscape.

The options for data transfers

The GDPR contains the general principle that any data transfers to third countries must ensure 'a high level of protection of personal data' and sets out a number of options by which this can be achieved. These options can be grouped (in descending order of preference) into the following three categories:

- adequacy decisions;
- appropriate safeguards; and
- derogations.

Adequacy decisions

Article 45 of the GDPR empowers the European Commission to adopt decisions that a third country (or a territory or sector within a country or an international organisation) provides an 'adequate' level of data protection that is comparable to that within the EU either through the country's domestic law or its international commitments. Generally speaking, no special authorisation or measures are required to transfer personal data to such countries.

To date, the Commission has adopted adequacy decisions under the Data Protection Directive (Directive 95/46/EC) in respect of Switzerland, Andorra, the Faroe Islands, Guernsey, Jersey, the Isle of Man, Argentina, Canada (partially), Israel, New Zealand, Uruguay and the US (albeit in the form of the Privacy Shield, which is not a general adequacy decision).

The Commission has recently announced that a review of all twelve existing adequacy decisions is under way. This comes shortly after the Commission's first annual review of the Privacy Shield, which was generally positive, but did recommend some tweaks at the US end to enhance the level of data protection provided. The Commission has also been in recent negotiations with both Japan and South Korea with a view to adopting further adequacy decisions. India too has expressed interest.

As part of the ongoing Brexit negotiations, the UK has stated its preference for an adequacy decision to facilitate the free transfer of personal data between the EU and the UK post-Brexit. However, this outcome is far from guaranteed. Even if the UK adopts the GDPR word-for-word, this may not be sufficient to ensure that it is granted an adequacy decision for several reasons.

> ***"Once the UK leaves the EU it may no longer be party to the EU Charter of Fundamental Rights — Article 8 of the Charter being the foundation on which much of the CJEU's recent data protection case-law is built. Consequently, data protection would no longer be expressly enshrined as a fundamental right under UK law."***

Firstly, even with a UK version of the GDPR on the statute-book, it is not certain that an equivalent level of data protection would be guaranteed in the UK given that the CJEU would no longer have jurisdiction over the UK legislation, and British courts would not be bound by CJEU case-law.

Secondly, once the UK leaves the EU, it may no longer be party to the EU Charter of Fundamental Rights — Article 8 of the Charter being the foundation on which much of the CJEU's recent data protection case-law is built. Consequently, data protection would no longer be expressly enshrined as a fundamental right under UK law.

Thirdly, aside from the GDPR, the UK's surveillance and data retention regime represents, in the words of the UK's Information Commissioner, 'a risk for a positive adequacy finding'. UK data surveillance and retention laws have drawn the ire of the CJEU long before Brexit. In December 2016, the CJEU ruled in *Secretary of State for the Home Department v Watson* that the UK's then domestic data retention legislation was incompatible with EU law (incidentally, David Davis MP, Britain's current Secretary of State for Exiting the EU was among the original claimants in that case).

In recent weeks, the UK's Investigatory Powers Tribunal has sent a further reference to the CJEU on the acquisition and use of so-called 'bulk communications data' by British security and intelligence agencies. An unfavourable CJEU ruling would weaken the claim for an adequacy decision. For these reasons, both the Brexit negotiations and data transfers to the UK should be kept under close review over the months ahead.

Appropriate safeguards

Article 46 of the GDPR allows for transfer of personal data to third countries that do not have adequacy status where the controller and processor have provided 'appropriate safeguards'. Such safeguards must include 'enforceable data subject rights and effective legal remedies for data subjects'. Of the safeguards, the most widely used mechanisms under the existing Data Protection Directive are standard contractual clauses ('SCCs') and binding corporate rules ('BCRs').

SCCs are a set of European Commission approved contractual clauses that are to be incorporated into data transfer contracts between entities transferring personal data from within the EU to a third country that does not enjoy adequacy status. While SCCs require the data exporting and importing entities to fill in certain details relating to the personal data being transferred and the purposes of the transfer, the clauses themselves cannot be amended or contradicted by any other part of a data transfer agreement. The continued validity of SCCs as a mechanism to transfer personal data to third countries (specifically the US) has been called into question by the Irish High Court's recent decision in the 'Schrems II' case.

On an application from the Irish Data Protection Commissioner ('DPC'), the High Court accepted the DPC's

(Continued on page 12)

(Continued from page 11)

'well founded concerns' surrounding the adequacy of the right to redress for European data subjects when their data are transferred to the US. The High Court is to send a preliminary reference to the CJEU. The DPC's concerns centred on the restrictive standing rules which make it 'exceedingly difficult' for EU data subjects to bring a data protection claim before the US courts. While the High Court ruling casts doubt on future use of SCCs as a mechanism to transfer personal data to third countries, it is unlikely that any such CJEU ruling will issue for at least a year. Although these developments should be closely monitored by data controllers that rely on SCCs to transfer personal data, SCCs remain a valid data transfer mechanism pending any CJEU ruling in Schrems II. The article on pages 13-14 of this edition contains further commentary on the Schrems case.

BCRs represent an alternative mechanism for intra-group transfers of personal data. In effect, BCRs are a set of rules that are binding on each member of a corporate group engaged in 'joint economic activity'. BCRs must specify certain details relating to the personal data being transferred, and should include certain general data protection principles, which are set out in detail in Article 47 of the GDPR. BCRs are to be approved in advance of their use by the relevant data protection supervisory authority. However, given that BCRs are only available for transfers within the same corporate group, their application is generally limited.

Article 48 of the GDPR recognises a further mechanism to transfer personal data between the EU and a third country where a court, tribunal or administrative authority of a third country has taken a decision requiring the controller or processor to disclose certain personal data. Article 48 provides that such requests will only be 'recognised or enforceable' if based on an international agreement, such as a mutual legal assistance treaty ('MLAT') in force between the requesting third country and the EU and/or the relevant EU Member State.

The MLAT procedure has been in sharp focus recently as a result of the ongoing US litigation between Microsoft Corp. and the US government. In that case, US prosecutors are seeking to compel Microsoft through the US courts to disclose personal data held on a server located in Ireland. Microsoft contested the US court's initial warrant, arguing that because the information sought was located in Ireland it was beyond the territorial jurisdiction of a US warrant. Microsoft succeeded before the US federal Court of Appeals, which indicated that the appropriate avenue for the prosecutors to obtain the relevant evidence is through the relevant MLAT agreements. The US government has appealed and the case is listed for hearing in the current term before the US Supreme Court. The case should be monitored in particular by EU-based controllers with US parents / subsidiaries where personal data is stored within the EU.

Derogations

Article 49 of the GDPR provides a list of scenarios whereby personal data may be transferred outside the EU by way of derogation (i.e. where neither an adequacy decision nor appropriate safeguards are in place). It is clear from the text of the GDPR that this category is a last resort when it comes to transferring data to third countries. One method of derogation is where the data subject has provided their explicit consent to the transfer, having been informed of the possible risks inherent in the transfer due to the absence of an adequacy decision and appropriate safeguards.

Article 49 also recognises certain other situations where transfers can be made – including where the transfer is necessary to protect the vital interests of the data subject or a third person – but as a general rule the derogations contained in Article 49 should not be relied on as a part of a general data transfer policy. The exceptional rather than routine nature of the Article 49 derogations is further illustrated by Article 49's recognition that controllers may transfer personal data to a third country where necessary for the controller's 'compelling legitimate interests', provided that such transfers are not repetitive, involve only a limited number of data subjects and suitable safeguards have been put in place.

Final remarks

As the above demonstrates, the European data transfer landscape is constantly evolving. Controllers should keep a watchful eye on these developments to ensure that their data transfer practices are compliant but also in order to meet their transparency, record-keeping and compliance obligations under the GDPR. To do so, controllers need to understand both the ever-evolving data transfer landscape and where they fit within it.

Hugh McCarthy
Arthur Cox
hugh.mccarthy@arthurcox.com