European Court of Justice Decision Impacts on DIFC Data Protection

Nick O'Connell
N.Oconnell@tamimi.com - Riyadh

December 2015 – January 2016

Article 11 of DIFC Law No. 1 of 2007 (the "DIFC Data Protection Law") makes provision for the transfer of personal data to recipients located outside of the DIFC where such recipients are located in jurisdictions considered to provide an adequate level of data protection. Therefore, recipients located in the US who certify their adherence to the privacy principles issued by the US Department of Commerce in its Safe Harbour Policy ("Safe Harbour Policy") have previously been granted adequate protection status under the DIFC Data Protection Law and its Regulations. Following a recent decision of the European Court of Justice ("ECJ"),1 the DIFC Commissioner of Data Protection has issued guidance on the use of the Safe Harbour Policy as a basis for transferring personal data from the DIFC to recipients in the US.

What happened?

The ECJ decision invalidated an earlier European Commission Decision which found that entities compliant with the Safe Harbour Policy provided an 'adequate level of protection' in respect of personal data. Broadly speaking, if a US entity was compliant with the Safe Harbour Policy, European entities were able to transfer personal data to the US entity safe in the knowledge that the transfer was compliant from a European Union ("EU") data protection perspective. The recent ECJ decision means that, at least for the time being, European entities can no longer rely on a US recipient's compliance with the Safe Harbour Policy to ensure transfers of personal data to such entities meet EU requirements.

Why is this relevant to entities located in the DIFC?

Like some other jurisdictions, the DIFC Data Protection Law uses the EU's approach to identifying jurisdictions that are 'safe' from a data protection perspective. Now that US entities in compliance with the Safe Harbour Policy are no longer deemed safe by the EU, the DIFC Commissioner of Data Protection has had to reconsider whether such entities should still be considered safe from a DIFC Data Protection Law perspective.

What needs to be done?

The DIFC Commissioner of Data Protection has noted that there are on-going negotiations between the EU and the US to try to address the issue. In the meantime, entities located in the DIFC that transfer personal data to the US should review the legal basis for such transfers to ensure continued compliance with DIFC Data Protection Law requirements.

What about other jurisdictions in the Region?

The Qatar Financial Centre ("QFC"), which has its own data protection regime similar to that of the DIFC, was not affected by this development. Instead of relying on a specific list of jurisdictions that are deemed to provide an adequate level of data protection, the QFC relies on more general principles. These generally provide that a data controller may only transfer personal data to a recipient located in a jurisdiction outside the QFC if an adequate level of protection for that personal data is ensured by laws and regulations that are applicable to the recipient. The adequacy of the level of protection ensured by such laws and

regulations is assessed with reference to all the circumstances surrounding the personal data transfer operations, including the nature of the data, the purpose and duration of the proposed processing operations, the country of origin and country of final destination of the personal data. Any relevant laws to which the recipient is subject, including professional rules and security measures, are also considered. As a result, it has not been necessary for the QFC to explicitly exclude recipients in compliance with the Safe Harbour Policy in a manner similar to that taken by the DIFC Commissioner.

Abu Dhabi Global Market ("ADGM"), a new financial services free zone established in the emirate of Abu Dhabi, has recently issued a European-style data protection regime based largely on the DIFC Data Protection Law. It contains requirements relating to the processing of personal information, including the transfer of personal information out of the ADGM free zone, and provides for a complaint process and penalties for non-compliance. Interestingly, ADGM issued its Data Protection Regulations on 21 October 2015 — just weeks after the relevant ECJ decision on the Safe Harbour Policy. Despite this, ADGM's lists of jurisdictions designated by the ADGM's Registrar as providing an adequate level of data protection include 'United States of America, subject to compliance with the terms of the applicable US-EU or US-Switzerland Safe Harbours'. The qualified nature of this reference would seem to exclude the Safe Harbour Policy for the time being, while there are no 'applicable' US-EU or US-Switzerland Safe Harbours in place.

Conclusion

If you are a DIFC-based entity transferring personal data to the US, and you have not yet reviewed the legal basis upon which you are relying to justify such transfers, then you should do so in order to ensure continued compliance with DIFC Data Protection Law requirements.

Endnotes

1. Case C-362/14, Maximillian Schrems v Data Protection Commissioner. Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises on data protection, including data transfer related issues. For further information, please contact Nick O'Connell – n.oconnell@tamimi.com.