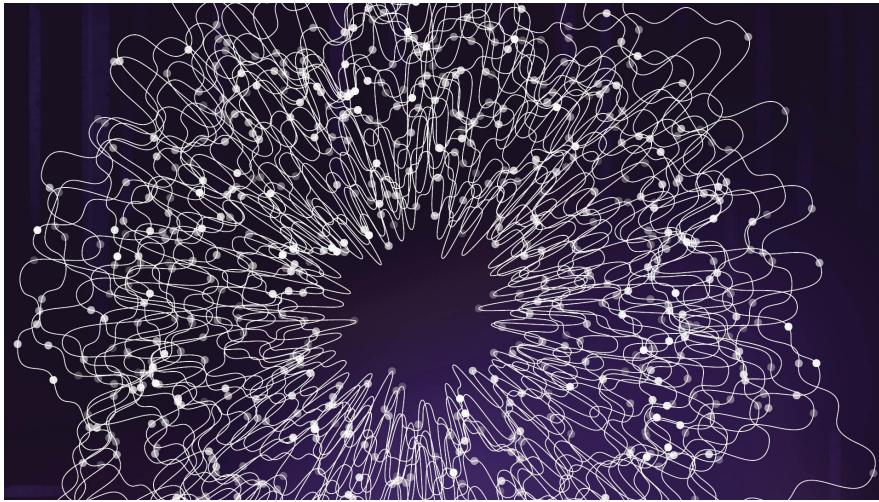


Schrems II: implications for data transfers from the GCC?

Nick O'Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data
n.oconnell@tamimi.com - Riyadh

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi



The European Court of Justice's recent "Schrems II" decision (case C-311/18) has attracted a lot of attention in data protection circles. One of the key outcomes of the decision is that it removes one of the grounds upon which European entities could legitimately transfer personal data to certain entities in the United States.

So, what relevance does a European court decision, relating to Europe's General Data Protection Regulation and an arrangement between the EU and the US Department of Commerce, have on personal data processing operations in the GCC? That's a very good question.

Context

Modern data protection laws typically restrict transfers of personal data to recipients in other jurisdictions, unless it can be shown that those other jurisdictions offer a similar level of protection to personal data as applies in the originating jurisdiction. If there were no restriction of this nature, then data protection rules in the originating jurisdiction could be undermined, simply by transferring personal data to a jurisdiction that does not have similar high standards.

Some jurisdictions issue a list of jurisdictions that they consider to provide an adequate level of data protection. Transfers of personal data to recipients in such jurisdictions are permitted. In contrast, transfers of personal data to other jurisdictions would only be permitted if the responsible data controller can show that the proposed transfer falls within another justification set out in the relevant data protection law.

The United States does not have a generally applicable data protection law. Accordingly, it is not considered a jurisdiction that provides an adequate level of protection to personal data. For this reason, the US was not on Europe's list of jurisdictions to which personal data could be transferred without the need to meet one of the other justifications set out in the data protection legislation.

Noting that the transfer of personal data between the EU and the US was likely to be important, effort was made at a governmental level to establish a reliable mechanism. This resulted in an arrangement between the EU and the US Department of Commerce, whereby US entities could undertake to comply with data protection criteria issued by the Department of Commerce. This arrangement, known as 'Safe Harbor', established a mechanism by which transfers of personal data to such specific US entities would be treated as transfers to entities in a jurisdiction that provided an adequate level of protection to personal data.

In October 2015, the legitimacy of the Safe Harbor mechanism was rejected by the ECJ in "Schrems I" (case C-362/14). The ECJ concluded that Safe Harbor did not guarantee that personal data transferred to recipients in the US would enjoy the same level of protection as it enjoyed in Europe. As a result, EU data controllers who had previously relied on Safe Harbor to justify personal data transfers to recipients in the US had to scramble to find an alternative justification.

Again, noting the importance of the transfer of personal data between the EU and the US, an effort was made, at a governmental level, to establish an alternative mechanism. This resulted in the establishment of an approach referred to as the 'Privacy Shield'. The specific differences between the Privacy Shield and Safe Harbor are not material for present purposes. It *is* material that the legitimacy of the Privacy Shield was subsequently challenged on the basis that it did *not* provide an adequate level of protection to personal data transferred to the US. In Schrems II, the ECJ threw out the Privacy Shield as a legitimate basis for transferring personal data to the US.

How is this relevant to the GCC?

In general, the concept of data protection is relatively new to the Gulf Cooperation Council countries, Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE. At the time of writing, only Bahrain and Qatar have nationally applicable data protection laws of general application. Two free zones in the UAE (Abu Dhabi Global Market ('ADGM') and Dubai International Financial Centre ('DIFC')), and a licensing authority in Qatar (Qatar Financial Centre ('QFC')), also have modern data protection regimes.

In the other jurisdictions (Kuwait, Oman, Saudi Arabia, and 'mainland' UAE), there are not currently any modern data protection laws of general application. (There are provisions that touch on data protection concepts, but these are not of general application, and not relevant for present purposes.) In this context, the Schrems II decision does not really change anything; data controllers operating in these jurisdictions would not have (legitimately) been relying on the Privacy Shield to justify personal data transfers to the US.

Amongst Bahrain, Qatar, ADGM, DIFC, and QFC, the respective laws and regulations provide for what can be understood as a 'traditional' approach when it comes to transfers of personal data to recipients located outside the respective jurisdictions. Generally, such transfers are prohibited unless the recipient is located in a jurisdiction that provides an adequate level of data protection or some other justification is available in the relevant law or regulations.

Bahrain and Qatar

For Bahrain and Qatar, the situation is such that, although the respective data protection laws contemplate that local data protection authorities will issue their own lists of jurisdictions they deem to be adequate, neither of these data protection laws is fully operational. At the time of writing, no such lists have been issued, so Schrems II is of no real consequence; no one in Bahrain or Qatar has been relying on the Privacy Shield as a basis of personal data transfers to the US.

Abu Dhabi Global Market

In contrast, ADGM's Personal Data Regulation 2015 specifically contemplates the application of the Privacy Shield as a mechanism for justifying the transfer of personal data to recipients in the US. The US is listed in ADGM's list of jurisdictions deemed to provide an adequate level of personal data protection, with the note, 'subject to compliance with the terms of the EU-US Privacy Shield'.

So, what does this mean for those data controllers, subject to the ADGM's Personal Data Regulation 2015, who have been relying on the Privacy Shield as the legal basis for transfers of personal data to the US?

In our view, as Schrems II has rejected the legitimacy of the Privacy Shield, it would not be correct for the same mechanism to continue to be recognised by ADGM. The wording of the note in the ADGM regulation itself is sufficient to conclude that, when the Privacy Shield was rejected by the ECJ, it was no longer a legitimate basis for personal data transfers from ADGM to the US pursuant to the ADGM Data Protection Regulations 2015.

We anticipate that ADGM's Office of Data Protection will issue a confirmation to this effect in the near future. Regardless, data controllers in ADGM who have been relying on the Privacy Shield will promptly need to establish an alternative basis to ensure that their transfers of personal data to the US are compliant with ADGM requirements.

Dubai International Financial Centre

For the DIFC, at the time of Schrems I (i.e. prior to October 2015), transfers of personal data to US entities registered with the US Department of Commerce pursuant to the Safe Harbor mechanism were treated as transfers to a jurisdiction with an adequate level of protection. In October 2015, the DIFC Commissioner of Data Protection was swift to act in removing Safe Harbor as a basis for the legitimate transfer of personal data to recipients in the US. At that time, DIFC licensed data controllers needed to identify an alternative basis for transferring personal data to recipients in the US. Notably, when the Privacy Shield became available, DIFC did not explicitly adopt it as an alternative.

In the new DIFC Data Protection Law 2020 (which came into law on 1, July 2020), the application of the Privacy Shield was specifically excluded. The explanation given in the law is that the DIFC does not have its own Privacy Shield arrangement with the US Department of Commerce.

Against this background, Schrems II should have no effect on data controllers subject to the DIFC Data Protection Law 2020. Such data controllers were not able to rely on the Privacy Shield from the outset. Any data controllers that have (erroneously) been transferring personal data to the US in reliance on the Privacy Shield mechanism should promptly review their personal data processing activities. (The same can be said for those who may still think that Safe Harbor applies.)

Qatar Financial Centre

QFC is in a slightly different position to both ADGM and DIFC. The QFC Data Protection Regulation 2005 contemplates a distinction between transfers to jurisdictions that ensure an adequate level of protection of personal data, and transfers to jurisdictions that do not. Despite this, it does not actually maintain a list of such 'adequate' jurisdictions.

The QFC approach could be understood as involving something of a 'self-assessment' on the part of the data controller. Data controllers need to assess all the circumstances surrounding personal data transfer operations, including: the nature of the data; the purpose and duration of the proposed processing; the

origin and final destination of the personal data; and any relevant laws to which the recipient is subject, including professional rules and security measures. Taking this into account, they may reach the conclusion of adequacy in respect of the recipient's jurisdiction.

Now, following Schrems II, those QFC data controllers who considered the Privacy Shield as part of their self-assessment will need to reconsider whether all the other circumstances around their personal data transfers to the US will still support a conclusion of adequacy in respect of the recipient's jurisdiction.

What next?

The data protection landscape in the GCC continues to develop, and it is important to keep monitoring it. With regard to the Schrems II decision in particular, data controllers who are subject to the data protection requirements of ADGM in Abu Dhabi and QFC in Qatar are well advised to review the basis upon which they justify the transfer of personal data to the US. If the Privacy Shield played any role, then alternative grounds need to be identified in order for further transfers to be compliant on this point.

For further information, please contact Nick O'Connell (n.oconnell@tamimi.com) or Andrew Fawcett (a.fawcett@tamimi.com).