EU-US Privacy Shield is no more. What now for employers After Schrems II?

27 July 2020

The Court of Justice of the European Union (CJEU) has given its preliminary ruling in Schrems II - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case C-311/18) in which it strikes down the EU-US Privacy Shield as a mechanism for transferring employees’ personal data to the US, on the basis that the adequacy of the protection provided by the Privacy Shield is not sufficient.

This decision is of utmost importance to all companies transferring data outside of Europe – but particularly those companies who have been transferring data to the United States and relying on Privacy Shield as the basis for doing so.

What does the law say and what’s changed?

The General Data Protection Regulation (GDPR) restricts the transfer of European employees’ personal data outside of the EEA unless the rights of individuals in respect of their personal data are protected. “Transfer” here is a slightly misleading term, as this includes moving personal data to another company within the same corporate group as well as those situations where employee data can be viewed or accessed by others in the same company who sit outside of Europe.

Companies are permitted to make these transfers if certain mechanisms are in place, as set out in the GDPR. In respect of transfers to the United States, one of the applicable mechanisms was the EU-US Privacy Shield framework.

By way of background, Privacy Shield replaced the previous EU-US agreement known as Safe Harbor. The Safe Harbor scheme was challenged by the same claimant in the CJEU (Mr Maximillian Schrems) and, as a result, was held not to provide sufficient protection for the personal data rights of European data subjects. Privacy Shield was intended to address and remedy the Court’s concerns in that first case.

In this second judgment, it has been held that the US legal regime which governs access to personal data by security bodies continues to provide inadequate safeguards for European data subjects. Further, it was found that EEA citizens may not be able to obtain an adequate judicial remedy if their personal data is not as well protected as it would be in the EEA. As a result, the CJEU has held that the Privacy Shield framework suffers from the same issues as Safe Harbor and is not a suitable basis on which to make transfers of personal data to the United States.

In practice, this means that organisations will no longer be able rely on the Privacy Shield framework to provide a lawful basis for the transfer of personal data to the United States.

Why is this important?
Transfer of employee personal data from the UK (and other EEA countries) to the United States is commonplace. Employers outsource elements of their employee administration, such as payroll, to US entities. Where a merger, acquisition or re-organisation occurs with the involvement of a US parent, it is likely to involve a transfer of British and European employee personal data to the United States. In addition, it is often the case that data servers are based in the United States.

In order to take these actions going forward, employers are required to ensure that one of the GDPR mechanisms are in place and there is now one less mechanism available to them to do so.

**What can employers do?**

As mentioned above, the GDPR does contain other mechanisms to allow the transfer of data to countries outside of the EEA. Employers will need to ensure that they put one of these alternative solutions in place. Although the Information Commissioner’s Office (ICO) in the UK has said (for now) that companies currently using Privacy Shield may continue to do so, our recommendation would be to take steps to review EU-US data transfers and consider an alternative solution going forward.

These possible alternative mechanisms include:

- **Standard data protection clauses adopted by the European Commission**: Known as ‘standard contractual clauses’ (SCC) or sometimes ‘model clauses’. SCCs must be entered into by the data exporter (based in the EEA) and the data importer (outside the EEA). SCCs must be used in their entirety and without amendment. The European Commission has so far issued two sets of SCCs for data transfers from EU data controllers to data controllers established outside the EU or EEA and one set of contractual clauses for data transfers from controllers in the EU to processors based outside the EU or EEA. These clauses were also challenged by Mr Schrems and were upheld by the CJEU (although not unscathed, as set out further below).

- **Binding corporate rules (BCRs)**: These provide a code of conduct to govern the operation of data protection within a multinational group. They apply to restricted transfers of personal data from the group’s EEA entities to non-EEA group entities. BCRs must be submitted for approval to an EEA supervisory authority in an EEA country where one of the companies is based.

- **Additional circumstances**: The GDPR also provides a number of additional alternative lawful bases for the transfer of personal data where there is no adequacy decision and no SCCs, BCRs or other safeguards in place. For example, data exporters may transfer personal data where that processing is “necessary for the performance of a contract between an employee and an employer”. However, it is important to note that these additional bases are construed narrowly. In this example, it may be difficult to establish that data transfer is necessary for the performance of a contract in an employment context. In addition, the other data protection principles apply (such as purpose limitation and data minimisation), which may have an impact upon how much data an employer can collect and what it can do with that data in the first place.

**What about SCCs?**

Although SCCs have been validated in this CJEU decision, there may still be a degree of risk that SCCs may be open to challenge in the future. SCCs are intended to provide safeguards by which employers can ensure that GDPR standards apply once employees’ personal data leaves the EEA. But it is important to remember that they only bind a party to that agreement. As such, they cannot override local law or bind the actions of local state agencies in respect of potential violation of data subjects’ rights under the GDPR.

The Court emphasised in its judgment that that there is an obligation on data exporters (i.e. employers) and the recipient of personal data (the importer, which could be another group company or a supplier) to verify the level of protection in the recipient nation prior to any personal data transfer to that country. Indeed, the CJEU held that SCCs and other valid transfer mechanisms will only be lawful if they are verified on a case-by-case basis for each data transfer.

As a result, SCCs continue to be a valid mechanism for transferring personal data to countries outside the EEA but subject to limitations. The CJEU held that SCCs may not always constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to a third country, in particular where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.
The judgment reiterates the importance of businesses verifying, prior to any transfer, whether an appropriate level of protection is respected in the relevant third country. Where there are no appropriate safeguards, the transfer of personal data to that third country should be suspended by the exporter or, failing that, the relevant Member State data protection supervisory authority.

The verification assessment by data exporters and importers will need to take into account: the regulatory regime in the countries in which each are based; an assessment of the nature and purpose of the transfer; the extent to which the laws in the destination country provide adequate protection of data subjects’ personal data; any additional safeguards applied to the proposed transfer arrangements, and any residual risk to a data subject.

What next?

Now more than ever, it is critical for employers to assess the type of employee data they transfer outside of the EEA to those countries without adequacy decisions. Employers need to be clear as to the legal basis for the transfer of employee data.

With this in mind, businesses should analyse data flows which involve transfers of personal data outside the EEA and determine which transfer mechanism (Privacy Shield, SCCs, etc.) is currently being used. For those transfers relying upon Privacy Shield, an alternative transfer mechanism must be found as a priority.

For businesses using (or considering) SCCs, the level of appropriate safeguards provided by that transfer must be assessed in each case to determine whether SCCs are in fact suitable. This means looking at the real-life risks of the transfer and the use of the SCCs, within the context of the sector / industry and other relevant factors including the destination country and the identity of the recipient, which may be challenging particularly given the uncertainty in the CJEU’s judgment in relation to relying on SCCs for transfers of personal data to the United States.

Despite the questions that were raised by the CJEU, SCCs remain, for now, the most realistic option for the transfer of personal data outside of the EEA. We expect it will take time for the full practical implications of the decision to flow down and take effect.

Given the impact this decision will have on businesses, we expect Member State data protection supervisory authorities may delay commencing enforcement actions to enable businesses time to assess the situation and put in place alternative solutions, as happened following the 2015 Schrems I judgment and the invalidation of the Safe Harbor framework. However, a grace period is not guaranteed, nor would it prevent individuals from bringing private claims for compensation or group litigation claims.

DLA Piper is developing a methodology to assist our clients in navigating the impact of the judgment and carrying out the required test when relying on SCCs.

For further information and advice, please get in touch with DataPrivacy@dlapiper.com or your usual DLA Piper contact.