CLIFFORD
CHANCE

Briefing note 6 October 2015

Safe Harbor declared invalid – what it means for your business

The Court of Justice of the EU today published its judgment in the case of *Schrems v Data Protection Commissioner* (C-362/14), declaring the European Commission's decision on the EU/US "safe harbor" arrangement to be invalid.

This will have significant implications for transfers of European personal data to the US. European organisations making transfers, and US organisations participating in the safe harbor, need to be watching developments and developing their go-forward compliance strategies.

The safe harbor

EU data protection laws prohibit transfers of personal data to countries outside the European Economic Area which do not ensure "adequate" protection for the transferred data. The US safe harbor has until today been a key tool used by businesses to address this prohibition.

The EU Data Protection Directive allows the European Commission to decide whether particular countries ensure adequate protection. It has made adequacy jurisdictions in relation to a small number of countries.

In particular, the Commission decided in 2000 that the self-certifying "safe harbor" scheme administered by the US Department of Commerce provides adequate protection for personal data transferred to scheme participants.

Safe harbor participation requires a US organisation to sign up to a set of data protection principles, broadly based on the EU model, which are enforceable by the Federal Trade Commission. Some 4,400 US organisations, including many well known IT service providers, participate in the safe harbor and invite their European affiliates, customers and others to rely on it when sending their data to the US. Safe harbor reliance has become routine.

The *Schrems* case

The *Schrems* case concerns transfers of personal data from Facebook's Irish operation to the US, based on Facebook's safe harbor participation.

Facebook user Max Schrems complained to the Irish data protection authority that the safe harbor did not adequately protect his personal data, arguing that Facebook's transfers to the US should be prohibited unless stronger protections are put in place. Mr. Schrems is particularly concerned about access to his personal data by US security and other agencies.

Headlines

- US safe harbor declared invalid with immediate effect
- Huge numbers of on-going data transfers to the US may now be unlawful
- Data subjects may complain that their data has not been adequately protected
- Consider switching to model contracts for new – and possibly existing – transfers
- The European Commission may be able to solve the problem in the medium term
- Action required now to mitigate risk exposure
- Watch for developments and regulatory guidance

The Irish authority took the view that it had no discretion under the EU Data Protection Directive to second-guess the Commission's assessment of the safe harbor and could not, therefore, take any action.

Mr. Schrems took the matter to the Irish courts, which made a reference to the EU Court of Justice.

The judgment

The EC Court today decided:

- National data protection authorities can examine the adequacy of protection provided by third countries, but only the Court itself can ultimately declare a Commission judgment invalid.
- The safe harbor decision is invalid.
- The Irish authority should consider Mr. Schrems' complaint and decide whether to suspend Facebook's transfers to the US.

Although the Court found the decision invalid on relatively technical grounds, it also took the view that the US does not in fact ensure adequate protection for personal data transferred from the EU - in particular because of US governmental agencies' broad rights of access to data held by safe harbor participants.

The judgment is effective today. The safe harbor no longer delivers certainty, and transfers relying on it may be unlawful immediately. In theory, fines and other sanctions could be imposed.

Two steps to mitigate your risk

STEP 1: review and document safe harbor arrangements internally and with third parties

If you are relying, or have been planning to rely, on the safe harbor to justify transfers of personal data to the US you will need urgently to consider whether to continue to rely on the arrangement or to seek an alternative justification. Do you know what safe harbor arrangements currently exist within your business and with third parties? These should be tracked and documented. You should also assess the materiality of data transfers taking place – are they business critical / high risk?

STEP 2: consider your options

Your team should discuss the following options:

- Put in place "model contracts" between the European data exporter and the US data importer. The Commission's judgments on the model contracts remain valid and, according to *Schrems*, any challenge to their validity would need to be taken to the EU Court. These contracts are in standard form and are generally quick to implement, although some member states' regulatory filing or approval is required.
- Transfer within a set of approved "binding corporate rules". This solution, however, takes many months to implement and only applies to intra-group transfers.
- Take the view that, in all the circumstances of a given transfer, the US can be regarded as providing an adequate level of protection – this is the "do nothing" option, with associated risk – not recommended unless supported by regulatory guidance, or possibly in the case of very low risk transfers.
- In extreme cases you might consider bringing infrastructure onshore.

When planning next steps you will need to take account of the likely reaction of the European Commission and the US authorities to the Court's judgment. They have for some years been engaged in negotiations to strengthen the protection provided by the safe harbor, and have indeed reached agreement on a number of points. The timetable of these negotiations may now be accelerated, leading to a replacement judgment in the coming months. This may therefore turn out to be a short-term problem, with relatively modest risk of regulatory action until the Commission is able to make a new safe harbor decision, defensible before the Court.

Conclusions

These are early days. The European Commission, the national data protection authorities and the working party established under Article 29 of the EU DP Directive are likely to issue guidance over the coming weeks. The Commission has announced that it will seek to ensure consistent pan-European guidance, although in practice there are real variations in local law which will need to be taken into account.

It is clear, however, that organisations need to take immediate steps to assess the scope of their exposure to the safe harbor and to start developing a strategy to minimise the associated risks. In the short term, model contracts are likely to multiply. In the medium term, the European Commission will doubtless be looking to put in place a durable solution through its negotiations with the US. Until then, your risk exposure is increased.