Maximillian Schrems v. Data Protection Commissioner

Court of Justice of the European Union, C-362/14, 6 October 2015

In a landmark judgment the Court of Justice of the European Union ('CJEU') followed the Attorney General's opinion in ruling that the EU-US Safe Harbor cross-border data transfer mechanism that had served trans-Atlantic trade for the past 15 years is invalid.

The facts

Mr. Schrems is an Austrian privacy campaigner. Following Edward Snowden's revelations in 2013 concerning the extent of access by US intelligence and law enforcement agencies to personal data of European citizens held by US companies, Mr. Schrems complained to the Irish Data Protection Commissioner ('DPC') challenging Facebook's use of Safe Harbor to transfer personal data to the US. Mr. Schrems claimed that the Safe Harbor does not provide an adequate level of protection for EU personal data in the US. He asked that the Irish DPC examine the validity of the transfer mechanism and, if necessary, that it suspend Facebook's further transfers of personal data to the US. The DPC refused to do so, on the basis that the transfers relied on an adequacy decision of the European Commission. The DPC considered it had no authority to review or challenge an adequacy decision of the Commission. Further, the DPC noted that there was no evidence that Mr. Schrems' personal data had, in fact, been accessed by US intelligence and law enforcement agencies.

Following the DPC's rejection of his complaint, Mr. Schrems appealed to the Irish High Court. The High Court found that while the US National Security Agency's electronic surveillance and interception of EU personal data "serve necessary and indispensable objectives in the public interest," Edward Snowden's revelations demonstrated a "significant over-reach" by the federal agencies. The Irish High Court noted that EU citizens have no right to be heard on these issues in the US, and that once transferred to the US, the data of EU citizens could be subject to "indiscriminate surveillance and interception carried out […] on a large scale […] contrary to the principle of proportionality." The High Court considered that the Commission's adequacy decision on Safe Harbor (Decision 2000/520) did not satisfy the right to respect for private life, as guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union, and noted that Mr. Schrems' case, in effect, challenged the legality of the Safe Harbor framework itself.

Accordingly, the Irish High Court decided to stay the proceedings and seek a preliminary ruling from the CJEU as to whether the Irish DPC was bound by the Commission's adequacy decision on Safe Harbor (Decision 2000/520), precluding any investigation by the DPC into the protection afforded to data transferred in reliance on Safe Harbor. Alternatively, the CJEU was asked to consider whether the DPC could conduct its own investigation into the continued adequacy of Safe Harbor, in light of the facts revealed since the Commission reached its decision.

The CJEU's judgment

In a judgment that concurred with the Opinion of Advocate General Bot, the CJEU decided that national data protection authorities ('DPAs') are not bound by Commission adequacy decisions, but are entitled to conduct their own investigation into whether transfers of personal data are subject to an adequate level of protection. In addition, the CJEU went further than the specific questions referred to it, and considered whether Decision 2000/520, on which the Safe Harbor rests, is valid. The CJEU decided that it is not.

In reaching its decision, the CJEU emphasised that until such time as a Commission decision is declared invalid by the CJEU, it must be presumed to be lawful. Member States and supervisory authorities cannot simply adopt measures contrary to Commission decisions. Rather, to ensure legal certainty, it is for the CJEU "alone" to decide that measures of the European institutions are invalid. The CJEU was clear that neither the Irish DPC, nor any other EU DPA, could simply declare the Safe Harbor to be invalid. However, DPAs are required to consider complaints from individuals concerning the protection of their rights and freedoms where data have been transferred abroad for processing.

Next, the CJEU proceeded to assess the validity of Decision 2000/520. Here, the court focused on the requirement that a third country must ensure an "adequate" level of data protection. In examining the concept of adequacy, the CJEU was clear that this does not require a third country to ensure a level of protection for personal data that is "identical" to that guaranteed in Europe. Instead, the level of protection for fundamental rights and freedoms must be "essentially equivalent" to that guaranteed in Europe. This will be a factual issue in each case, requiring examination of a country's domestic law and its international commitments. Further, as the levels of protection may change over time, the CJEU considered that the Commission would need to "check periodically" whether an adequacy finding remained "factually and legally justified."

In assessing the continued validity of Decision 2000/520, the CJEU noted, in particular, the fact that under the Safe Harbor, "'national security, public interest or law enforcement requirements' have primacy over the safe harbor principles," and (in effect) the fundamental rights of EU citizens in relation to their personal data.

The CJEU noted that Decision 2000/520 contains no reference to limitations on such interference, or effective legal protections against interference, and that this assessment is reflected in the Commission's own review of Safe Harbor. The CJEU was particularly critical of the absence of any limits on the access rights of US public authorities, or on their subsequent use of data. In the CJEU's view, "access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." Further, the CJEU considered that the absence of any process to enable an individual to pursue a legal remedy to seek access to, to rectify or to request the erasure of their data failed to respect the fundamental EU right to judicial protection.

Impact of the judgment

Immediately following the judgment, there were numerous exaggerated headlines and media sound bites, some of which went as far as to predict the demise of trans-Atlantic trade. Part of the cause for panic appears to have been a lack of understanding within organisations of the fact that alternative data transfer mechanisms are available. In addition, the absence of concrete guidance from government agencies and regulators may also have played a part. In many quarters, the CJEU's decision appears to have been a surprise, with commentators noting ahead of the judgment that it was inconceivable that the Safe Harbor would be allowed to fail.

Shortly after the judgment was given, the European Commission gave a media briefing in which First Vice President Timmermans and Commissioner Jourova welcomed the CJEU's reaffirmation of the fundamental rights of EU citizens, and emphasised that they are continuing to work with US authorities to address the shortcomings of the Safe Harbor. A further statement is expected once the Commission has had an opportunity to consider the full implications of the judgment.

Amongst the regulator community, the UK's Information Commissioner's Office ('ICO') was the first DPA to comment. Deputy Commissioner David Smith acknowledged that it will take time for those affected by the decision to assess their position, and implement an alternative transfer mechanism. The statement infers that the ICO will allow companies a period of grace before it commences enforcement actions. Anecdotally, it is said that other DPAs have already received complaints, and are considering how to respond. The first enforcement action may come from one of the countries in which there has been long-standing concern about Safe Harbor, or perhaps from a jurisdiction in which the DPA has no discretion as to whether to investigate a complaint.

What is the likely scope of further complaints? Initially, complaints may be made about specific transfers, but it seems only a matter of time before there are complaints about other data transfer mechanisms. This goes to the crux of the issue. The complaint that lies at the heart of Mr. Schrem's case is really a complaint about foreign law enforcement access to EU personal data. This is a political issue that requires a political solution. The data protection regime is not intended to address this. The Data Protection Directive (95/46/EC) looks to Member States to adopt their own legislative measures to address data processing for national security, defence and law enforcement purposes.

Arguments that can be made to challenge the Safe Harbor can be raised, to some extent, in relation to some of the other transfer mechanisms. Perhaps anticipating this, the CJEU was careful to state that it is for the Court alone to determine the validity of a data transfer mechanism. This may calm things for a period, but it is possible that the issue may return to the CJEU, in the context of a different data transfer mechanism, for further consideration.

Practical next steps

In the interim, what should organisations do? The starting point for most organisations will be to identify and assess their trans-Atlantic data flows. For some, their intra group data transfers will be a key focus. For other organisations, including non-US companies, reviewing transfers to third party vendors that have, until now, relied on Safe Harbor will be a priority. Once organisations have identified their relevant data flows, they will need to assess them. Flows that are fundamental to the business should be prioritised for review. Organisations will need to consider the nature and structure of the data flows in order to determine which data transfer mechanism will be most appropriate.

As regulators have been quick to note, several data transfer mechanisms are available. Depending on the underlying facts, the derogations at Article 26(1) of the Directive may offer a solution. Transfers that are necessary for the performance of a contract between the data subject and the controller, or for the implementation of pre-contractual measures taken in response to the data subject's request are permitted, as are transfers that are necessary for the

conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party. Transfers are also permitted with the unambiguous consent of the data subject. While derogations should not typically be relied on for systematic, ongoing transfers, they may play an important role in the context of a broader data transfer strategy. Aside from the derogations, binding corporate rules ('BCRs') or the Commission-approved standard contractual clauses may be appropriate.

Organisations transferring personal data from the UK should note that the Data Protection Act 1998 permits data transfers on the basis of an internal, case by case, adequacy assessment conducted by the data exporter. This option is not available in other jurisdictions.

Each of these alternative transfer mechanisms has its advantages and disadvantages. For many organisations, a combination of mechanisms to cover specific flows or data processing activities is the best solution. Organisations that had relied on Safe Harbor for their intra group transfers may decide that the effort required to transform their Safe Harbor certification into a controller-BCR is relatively modest. Safe Harbor-certified vendors may turn to processor-BCRs. The key issue is to understand the factual context before deciding on the right mechanism. All of the mechanisms have a cost associated with them. Some mechanisms, such as BCRs, require time to secure DPA approval. In the case of standard contractual clauses, the clauses may need to be filed or lodged with DPAs for approval, or DPA registrations may need to be updated to include the new data transfer mechanism.

The responsibility for finding an alternative data transfer mechanism rests on the shoulders of the European exporting controller, which will have the legal obligation to ensure that data are protected by adequate safeguards. In practice, processors may wish to seize the initiative and offer an enterprise-wide solution to their customers. Several US vendors have been prominent in facilitating replacement transfer mechanisms, making model clauses available for their EU customers to sign and return. Their EU customers will then need to complete the formalities of filing or lodging the clauses with EU DPAs. Parties will also need to consider whether any additional contractual amendments will be required to existing services agreements.

It remains to be seen whether regulators will offer any additional concessions to companies that seek to transform their Safe Harbor certification into something else. While the Safe Harbor has been criticised, in practice US companies that are part of the Safe Harbor take their compliance obligations seriously. These companies tend to have a robust and thorough approach to reviewing the adequacy of their data protection programmes ahead of the annual renewal of their Safe Harbor certification. Other data transfer mechanisms do not mandate an annual review in the same way that Safe Harbor did.

Other practical issues are also being grappled with. In the US, companies are unsure whether to continue with the renewal of a Safe Harbor certification that is due, or what steps to take in relation to data that has been collected on the basis of Safe Harbor. Guidance on these issues is awaited from the US Department of Commerce, but for now most companies appear to be maintaining their Safe Harbor certifications.

Looking forward

It is still not clear whether Safe Harbor 2.0 will rise, phoenix-like, from the ashes of the original Safe Harbor. Negotiations to improve the US-EU Safe Harbor Framework between the European Commission and the US Department of Commerce have been ongoing for some time, but 'Safe Harbor 2.0' has not yet been agreed. In responding to the *Schrems* case the Department of Commerce declared itself ready to work with the Commission to "address uncertainty created by the court decision so that the thousands of US and EU businesses that have complied in good faith with the Safe Harbor and provided robust protection of EU citizens' privacy in accordance with the Framework's principles can continue to grow the world's digital economy." There are rumours that discussions may already have re-started in earnest. Otherwise, the Article 29 Working Party is due to meet in plenary on 15 October to seek a coordinated response among DPAs. The Working Party is expected to issue guidance shortly.

In the interim, organisations that relied on Safe Harbor, either for intra-group transfers, or for transfers to service providers, must seek alternative mechanisms. Although the landscape remains unclear, there are steps that organisations should already be taking to assess their position and consider alternatives. There remains a great deal of uncertainty as to how these issues will be resolved, and organisations would do well to maintain a watching brief.

Bridget Treacy Partner
Lisa Sotto Partner
Hunton & Williams LLP, London and New York
btreacy@hunton.com
lsotto@hunton.com