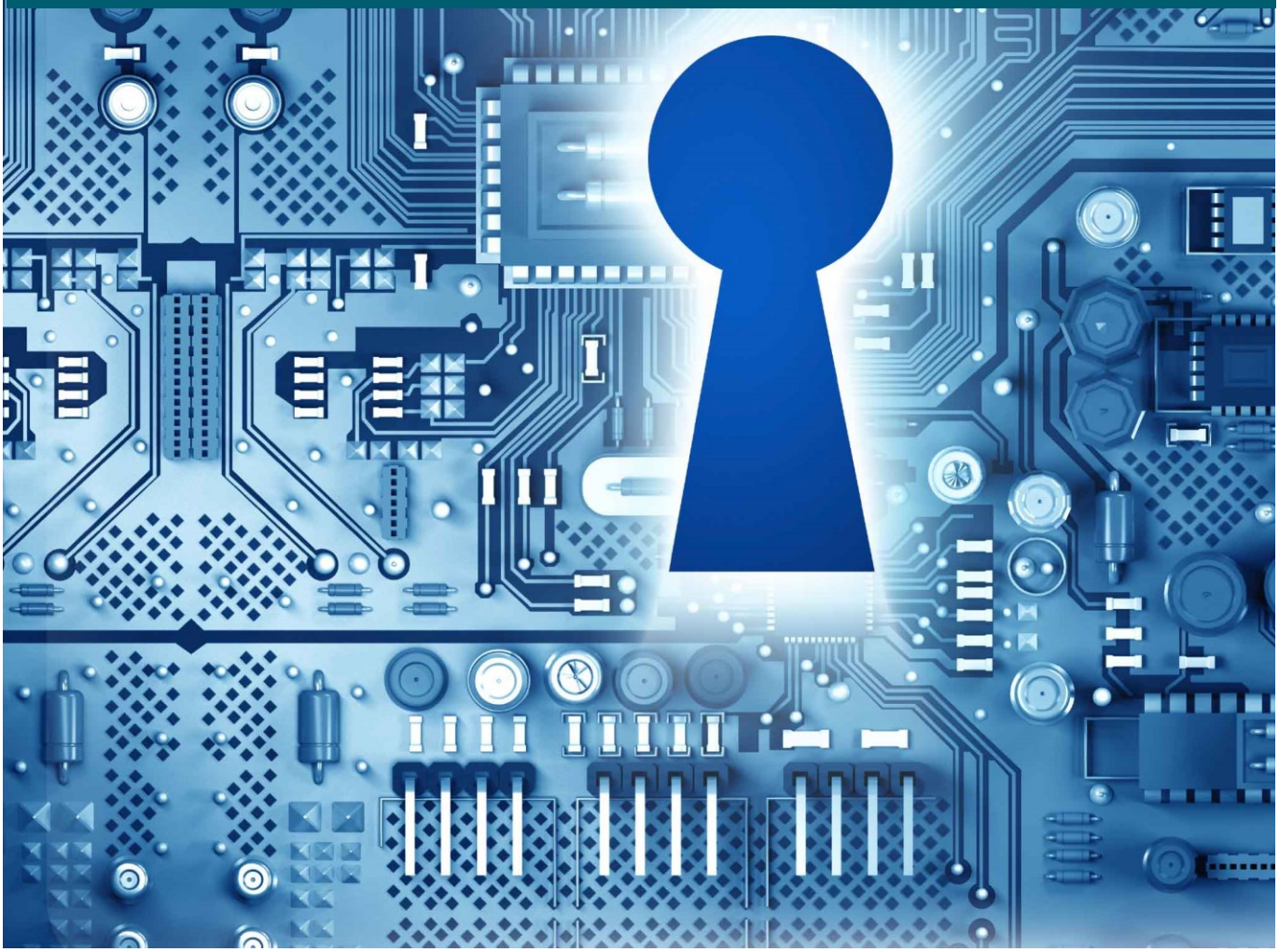
14 October 2015

US data transfers: practical next steps in the wake of Safe Harbor

OLSWANG



US Data Transfers: Don't panic! Practical next steps in the wake of Safe Harbor

You will already have heard about last week's *Schrems* decision in which Europe's highest court, the CJEU, invalidated the Safe Harbor scheme. The scheme had previously been relied on by over 4000 US organisations and countless more EU group companies and counterparts to legitimise EU to US data transfers.

In the immediate aftermath of the ruling, the Commission has stated that transatlantic transfers can continue based on the other available mechanisms, which remain valid. EU regulators are now considering next steps, with further guidance expected shortly from Europe's influential Article 29 Working Party.

These FAQs focus on some practical questions that in-house lawyers and internal stakeholders are likely to be asking in the interim.

What do I need to tell the Board? Is immediate action required? What is the risk level?

If your organisation has been relying on the US Safe Harbor, then, while we await guidance from the EU regulators, the decision creates uncertainty and potentially compliance risk.

- **Don't** panic. Enforcement risk is likely to remain low in the short term while regulators take stock of the decision and work out its implications. You have some breathing space to take stock of your exposure and plan your response.
- **Do** work out which of your suppliers are relying on Safe Harbor.
- **Do** consider whether there are any alternative mechanisms already in place that address adequacy requirements, such as model clauses and consent and, more unusually, binding corporate rules for processors.
- **Do** plan remediation for those suppliers where there is no valid mechanism in place.
- **Do** monitor what the regulators say over the next couple of weeks.

The true impact of this decision will depend on many factors - the size and resources of your organisation, and the scale and sensitivity of the data concerned. The reality is there is no "one-size-fits all" fix.

Frequently asked questions

When can we expect new guidance on this?

Shortly. The Article 29 Working Party, which is the body representing all national EU DPAs, met on 8 October and is due to meet again this week to begin work on a coordinated response.

Won't this situation just blow over?

The risk over transatlantic transfers will not be lifted completely until the EU's specific concerns about US law enforcement access to data have been fully resolved which is a much wider and more challenging political debate. The EU and US have been renegotiating "Safe Harbor 2.0" for some time. However this cannot be finalised until the US Judicial Redress Bill - designed to give EU citizens effective remedies – is adopted, and there is no certainty over when or if that will happen.

In the meantime, regulators and businesses cannot ignore the CJEU's finding that the Safe Harbor can no longer be relied upon. Doing nothing is not an option.

What is – or was - the Safe Harbor, and why is invalidation such a headache?

One of the principles of the Data Protection Directive is that personal data may not be transferred outside the EEA unless the destination country has an "adequate" level of legal protection. The Directive empowers the Commission to make a finding of adequacy for a particular non EEA country. Given the lack of comprehensive privacy legislation in the US, a general White List decision for the US was not an option. In 2000 the Commission issued an adequacy decision covering organisations registered on the US Government's Safe Harbor list. The scheme involves self-certifying compliance with the Safe Harbor Framework and annual renewal.

The scheme provided a neat compliance work around, both for US entities eligible to join, and for EU customer organisations and other contractual counterparts wishing to export data to them. Around 4000 importing organisations are currently registered, including major online platforms and cloud service providers. One can only guess at how many exporting organisations in the EEA are reliant on it. If Safe Harbor was the only basis on which those data transfers were compliant with the Data Protection Directive, its invalidation – with immediate effect – is a sizeable compliance headache.

What are the key legal points? Why has the CJEU ruled Safe Harbor invalid?

The CJEU ruled on these two points:

- Adequacy findings (like Safe Harbor) by the Commission are not a "shield" and do not prevent national DPAs from examining a data subject's claims that privacy protection in the destination country are not adequate.
- The Safe Harbor adequacy decision is invalid.

We look at the legal issues in more detail below – see "Legal analysis" below.

What does invalidation mean in practical terms? Could I face enforcement action?

Data transfers based solely on Safe Harbor violate EU data protection laws. This leaves the door open for investigations, sanctions and, in theory at least, fines by data protection authorities. Potentially, affected individuals may also be able to claim compensation.

With Safe Harbor protection invalidated, data exporters and importers need to ensure an alternative mechanism is in place to make transfers lawful once more. The Commission in its immediate response to the *Schrems* decision implies that US transfers based on alternatives – i.e. legitimising conditions including consent, and model contracts and BCRs – remain valid. The CJEU's ruling states that Commission decisions can only be invalidated by the CJEU, so these mechanisms remain valid for the time being. We look at these alternatives in more detail below.

How soon must I put an alternative in place? Will there be a grace period?

This is currently unclear. The ruling made Safe Harbor invalid with immediate effect. However, the regulators are themselves taking stock of the situation. The UK regulator the ICO has stated that it recognises that businesses

"will need some time" to review their transfer solutions. Europe's data regulators are working on a joined-up response. It is too early to say whether they will give businesses a specific grace period though there is unlikely to be either the resource or the political will to mount an extensive enforcement campaign in the short term. Provided your business is assessing exposure and planning and implementing alternative solutions, the risk of investigations, fines and sanctions is likely to remain low. Claims by individuals are possible, though haven't proved common to date for other breaches of data protection laws; private claims for compensation have tended to be confined to issues causing annoyance or distress such as spam.

What are the alternatives? What are the costs and what are the pros and cons?

Data transfer solution	Time and cost?	Any other considerations or pitfalls?
"Performance of a contract" condition	None, if it applies	It is worth looking into this option in certain scenarios. This option might, for example, work for US data controllers that collect personal data of EU data subjects via cookies or an app subject to EU law.
Consent condition	Depends on practicability	Has to be specific, informed and freely given – and some Member States require explicit opt-in consent, so this isn't the most practical of solutions. Plus, various data protection regulators have questioned consent for "massive" or "systematic" transfers. Plus, you need a technical solution for those individuals who say "no". For these reasons, consent is often helpful in combination with another mechanism but is problematic as a standalone solution.
EU model contracts	Relatively quick. Relatively inexpensive – compared to BCR	Very likely this will be the most favoured alternative to Safe Harbor at least in the short term as, although the *Schrems* decision leaves the door ajar for similar claims against Model Clauses, for the time being they are valid and ensure adequacy. May need to be filed with local DPA, depending on your jurisdiction, which adds to time and cost.
Binding Corporate Rules	Significant budget and lead time 12-18 months	Only available for intra group transfers or transfers to a qualifying processor Long lead time and costly to implement (at least 12-18 months) Not a viable short term fix for dealing with your supply chain save for those suppliers who are currently among the very few who have BCRs

Data transfer solution	Time and cost?	Any other considerations or pitfalls?
		for processors.
Self-assessment of adequacy	Quick. Inexpensive.	Not available in all Member States, though the ICO has referred to it as an option in its latest guidance on *Schrems*. May be viable for some transfers.
Use EU server or service provider	For providers, significant For EU customers, no cost and no delay	For providers and customers: If data is strictly separated, this solution is a very clean way to avoid EU data transfer issues. However, the solution only works if: • the EU server is operated and controlled by an EU entity; • data does not travel through the US; and • the US parent entity does not have any access to the data stored on the EU servers. The latter two requirements are often difficult to meet in practice. Also, data of multinational customers can often not be separated between EU and non-EU data. For providers: The decision to set up data centres in the EU should not just be data-driven. Corporate, EU law enforcement and tax law issues need to be considered too. That said, plenty of providers have already set up EU data centres.
Anonymise data	Depends on solution	It may be possible to avoid the transfer challenge completely by fully anonymising data before exporting out of Europe. The practical challenge is that it is increasingly difficult to fully anonymise data; it is often possible to reverse engineer back to identifiable individuals. Only exporting encrypted data may be another solution though again only if there is no means in practice for the importer to decrypt the data.

How have the major regulatory stakeholders reacted?

The Commission has welcomed the ruling as "*an important step for upholding Europeans' fundamental data protection rights*" and a vindication for the Commission's renegotiation of the Safe Harbor here.

The EU DPAs in the Article 29 Working Party have acknowledged the practical implications of this "milestone" decision and undertaken to provide a coordinated response here.

The UK ICO has sent a "don't panic" message to UK businesses advising them to wait and see.

In France, the CNIL's statement is quite reserved, stating that the CNIL raised the question of surveillance practice by US intelligence agencies several years ago and that it will soon be meeting with other Article 29 Working Party members "*to determine precisely the legal and operational consequences of this judgment on the entirety of transfers implemented under the "Safe Harbor"*.

In Germany, the German Federal Data Protection Commissioner and certain authorities, such as the Hamburg data protection officer, have published press releases welcoming the ECJ decision. Ominously they also announced that they will have a close look at the other data transfer vehicles, such as BCR and Model Clauses.

Olswang comment

Olswang's Data Protection Team have been analysing the impact of the decision. See comment by our team on the CJEU ruling in Data Guidance here, Handelsblatt here and on the AG's opinion which foreshadowed the ruling in Reuters here.

In more detail – the legal analysis

For readers with greater appetite for the ins and outs of the CJEU's ruling, the case raises some big picture issues: the interplay between fundamental EU rights and the data-gathering powers of overseas law enforcement and the relative powers and pecking order of the Commission, the courts and national DPA. It also raises fine points of detail about the specifics of the current DP Directive and the limits on the Commission's power to make findings that third countries provide adequate legal protection. The judgment is long and complex. What follows is a short and high level summary of the rationale underpinning the two key rulings in the judgment.

Powers of DPAs under Article 28 not fettered by a Commission adequacy decision

Paras 37-66 of the CJEU judgment

The key points to note about this part of the ruling include the following:

- The Directive requires DPAs to be independent and to monitor compliance with the Directive in order to guarantee data protection rights.
- Although DPAs' jurisdiction does not extend to processing carried out in a third country, in the case of a transfer to a third country the DPA does have jurisdiction over that part of the processing (eg the disclosure and transmission) taking place in the relevant exporting Member State. In other words the relevant DPA has power to check that the transfer from its Member State complies with the Directive.
- Measures of the EU institutions – like the Safe Harbor decision – are presumed to be lawful until they are annulled. Until a Commission decision is declared invalid, Member States and their DPAs cannot adopt measures contrary to that decision.
- However, a Commission adequacy decision cannot prevent an individual from lodging a claim concerning their DP rights and cannot eliminate or reduce powers given to DPAs by the Charter or the DP Directive.
- Acts of the EU institutions, like the Commission decision, cannot escape review of their compatibility with the law – in particular compatibility with the Treaty and fundamental rights of EU citizens.
- Only the CJEU (and not the national courts) can declare a Commission decision invalid.

The Safe Harbor Decision is invalid

Paras 67 -106 of the CJEU judgment

This turns on the conflict between data subjects' rights under the DP Directive and Articles 7 and 8 of the Charter and the breadth of US law enforcement powers to access data.

- **Article 1** of the Decision – which provides that compliance with the Safe Harbor Principles ensures an adequate level of protection – is invalid, without the need to examine the content of those principles. This is because:
  - They do not bind US public authorities, only self-certifying organisations.
  - The decision focussed on the adequacy of the Safe Harbor principles; not the adequacy of the wider US regime.
  - The decision expressly permits the Safe Harbor principles to be trumped by national security, public interest or law enforcement requirements.
  - The Decision does not refer to the existence of any limits on those powers or any legal protection against, or means of redress for, interference in privacy rights.
  - Under EU case law, interference with Charter rights must lay down safeguards, and any derogations must apply only as far as "strictly necessary".
  - The generalised nature of the US law enforcement access powers compromises Charter rights.
  - The US legislation does not provide individuals with the effective legal remedies required by the Charter.
  - The Decision did not state – as required by Article 25 of the Directive – that the US ensures an adequate level of protection.
- **Article 3** of the Decision – which sets out the rules of DPAs in the face of a Commission adequacy finding – is also invalid. This is because it purports to deny DPAs their powers under Article 28 to examine claims by a data subject about protection of his DP rights.

Contact

Ross McKean
Partner
London
+44 20 7067 3378

Sylvie Rousseau
Partner
Brussels/Paris
+32 2 641 1272

Dr Andreas Splittgerber
Partner
Munich
+49 89 206028-404

Blanca Escribano
Partner
Madrid
+34 91 187 1924

Brussels
+32 2 647 4772

London
+44 20 7067 3000

Madrid
+34 91 187 1920

Munich
+49 89 206 028 400

Paris
+33 1 70 91 87 20

Singapore
+65 6720 8278

Thames Valley
+44 20 7071 7300

OLSWANG

Olswang:
Changing Business

www.olswang.com