MAYER·BROWN

Update on the Court of Justice of the European Union's ruling on US Safe Harbor

What happens next?: Maximillian Schrems v Data Protection Commissioner C-362/14

Mark Prinsley
Partner
+44 (0)203 130 3900
mprinsley@mayerbrown.com

Kendall Burman
Counsel
+1 (202) 263 3210
kburman@mayerbrown.com

Oliver Yaros
Senior Associate
+44 (0)203 130 3698
oyaros@mayerbrown.com

27 January 2016

Speakers

Mark Prinsley is head of the Intellectual Property & IT group at Mayer Brown International LLP in London as well as the outsourcing practice. His practice involves acting for customers at all stages of outsourcing transactions. Recent outsourcing projects have included acting for a commodity exchange in the outsourcing of its IT functions; a telecommunications company in IT outsourcing; a global bank in the outsourcing of its human resources functions; a global chemicals company in outsourcing its finance and accounting functions; a global automotive company in the outsourcing of human resources functions; and a consumer goods company in Finance and Accounting outsourcing and the implementation of cloud computing arrangements and on privacy related matters. Mark also works on the technology transactions which generally include real-time licensing of financial markets data.

Kendall Burman is a Cybersecurity & Data Privacy counsel in Mayer Brown's Washington DC office. Prior to joining Mayer Brown she served in the administration of President Barack Obama, most recently as Deputy General Counsel for the US Department of Commerce. In that capacity, she served as the chief policy expert for the Office of the General Counsel, developing and executing the department's priorities in areas such as cybersecurity, consumer privacy, intellectual property and international trade. Previously, she served as Special Assistant to the President and Associate White House Counsel. In that role, her policy portfolio included science and technology, open government and intellectual property.

Kendall is a Cybersecurity Fellow at the New America Foundation and was a senior national security fellow at the Center for Democracy and Technology, where she examined issues at the intersection of civil liberties, national security and technology

Speakers

Oliver Yaros is a senior associate in the Intellectual Property & IT Group of the London office of Mayer Brown International LLP and advises clients on TMT, outsourcing, IT, data protection, privacy, e-commerce and IP issues. Oliver acts on global financial industry utility projects, IT and business process outsourcing projects and IT systems procurement transactions as well as advising a range of clients (financial institutions, manufacturers and retailers of consumer products, publishers and providers of digital media and online content) on many e-commerce and data protection issues. From May 2013 to October 2014, Oliver spent 18 months on secondment to the Global Banking and Markets Legal team of HSBC in London during which he advised HSBC on the creation of various global know your client / client onboarding and other types of banking industry utility joint ventures with other banks, on a number of multilateral and bilateral outsourcing projects, on investment banking IT system procurement projects and on various worldwide IP portfolio management and data protection issues.

Topics we will cover during this webinar

- An explanation of the decision
- Reaction to the decision in Europe
- Progress made in Europe and the US since the decision
- The 31 January 2016 deadline: What happens next and what steps should you take?

The Safe Harbor decision: The timeline

- In 1995, Data Protection Directive 95/46 is adopted to govern the processing of personal data in Europe.
- Under the Directive, export of personal data from the EEA to the US is prohibited unless levels of protection considered “adequate” by the European Commission are used.
- In 2000, the US Department of Commerce proposes a self certification “Safe Harbor” program under which US companies will process personal data received from Europe in compliance with the directive
- In Decision 2000/520, the European Commission decides that the US Safe Harbor program provides an adequate level of protection
- By 2015, about 4,500 companies have self-certified to Safe Harbor

Decision of the Court of Justice of the European Union

- The CJEU found that:
  - Decision 2000/520 does not prevent a national data protection authority from:
    - Examining a claim made by a person concerning the protection of his rights and freedoms with respect to the processing of personal data relating to him which has been transferred to a third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection; or
    - From exercising its rights to suspend transfers.
  - Member States have to be able to take the measures necessary to safeguard the fundamental right to the protection of personal data under the Charter of Fundamental Rights of the European Union

Decision of the Court of Justice of the European Union

- The CJEU found that:
  - Decision 2000/520 is invalid because:
    - In making its decision, the European Commission did not consider whether the US would ensure an adequate level of protection in Safe Harbor by reason of its domestic law or international commitments as required by the Directive;
    - Safe Harbor does not provide a guaranteed level of protection because:
      - US authorities may process personal data transferred to the US under Safe Harbor in a way that is incompatible with the purposes for which it was transferred there and beyond what is strictly necessary and proportionate for the protection of national security;
      - Safe Harbor certified organisations are required to comply with requests from US authorities; and
      - Data subjects have no right of redress.

Reaction to the decision

- Reaction from the UK Information Commissioner's Office (emphasis in bold):

  "…**We will now be considering the judgment in detail, working with our counterpart data protection authorities in the other EU member states and issuing further guidance for businesses on the options open to them**…Concerns about the Safe Harbor are not new. That is why negotiations have been taking place for some time between the European Commission and US authorities with a view to introducing a new, more privacy protective arrangement to replace the existing Safe Harbor agreement. We understand that these negotiations are well advanced. The ICO will be working with our European colleagues to produce guidance following the European Court of Justice ruling"

  6 October 2015

- Reaction from the UK Information Commissioner:

  "…**[We will not be] knee-jerking into sudden enforcement of a new arrangement.** We are coordinating our thinking very much with the other data protection authorities across the EU"

  8 October 2015

Reaction to the decision

- Reaction from the Article 29 Working Party:

"…the question of massive and indiscriminate surveillance is a key element of the Court's analysis**…the Working Party is urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights**…In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. **During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used**.

…**If by the end of January 2016, no appropriate solution is found** with the US authorities and depending on the assessment of the transfer tools by the Working Party, **EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions**.

…The Working Party considers that it is clear that **transfers from the European Union to the United States can no longer be framed on the basis [of Safe Harbor]… transfers that are still taking place…after the CJEU judgment are unlawful** "

16 October 2015

Reaction to the decision

- Reaction from the German Data Protection Commissioners (DSK):
  - **Transfers of personal data to the US solely under Safe Harbor are no longer permitted**
  - **The admissibility of data transfers to the US based on standard contractual clauses or binding corporate rules is also questionable**
  - The German DPAs will not issue any new permissions for data transfers to the US based on binding corporate rules or bespoke data export contracts for the time being
  - Under strict conditions, consent to the transfer of personal data to the US may be a viable basis [but] such data transfer must not occur repeatedly, on a mass scale or routinely. For the export of employee data or if data of third parties are affected at the same time… consent may be the basis for data transfers to the US only in exceptional cases
  - The European Commission is asked to insist on creating sufficiently broad guarantees for the protection of privacy in its negotiations with the US…**the decisions on standard contractual clauses must soon be adapted to the requirements laid down in the CJEU's ruling….for this reason the DSK welcomes the deadline of 31 January 2016 set by the Article 29 Working Party**

21 October 2015

Alternative methods of transferring personal data to the US

- Standard contractual clauses (data controller to data controller / data controller to data processor)
- Binding corporate rules
- “Ad hoc” / bespoke data export agreements
- Consent
- Other “derogations”
- EU Commission communications on the transfer of Personal Data from the EU to the United States (6 November 2015)
  - Supportive of the alternatives and implicit criticism of the challenges to the alternatives

Safe Harbor 2.0

- EU concerns about safe harbor emerged in 2010 (in Germany)
- Commission Communication on the Functioning of Safe Harbor from the perspective of EU citizens and companies established in the EU – November 2013
- Growth in businesses relying on safe harbor
  - Approx. 400 2004
  - Approx. 3200 2013
  - Approx. 4500 2015

EU concerns about Safe Harbor in 2013

- Lack of transparency
- Lack of redress
- Limited enforcement
- Access by US Authorities

EU position post Schrems

- Requirements for new Safe Harbor
  - Stronger oversight by the Department of Commerce
  - Clearer cooperation between the Department of Commerce and EU National Data Protection Authorities
  - More likelihood of enforcement by the FTC

US Position post Schrems

- US and EU had an understanding on most elements of a new Safe Harbor agreement before Schrems.
- Steps taken by the United States include:
  - Executive Action (Presidential Policy Directive PPD-28 – 17 January 2014)
  - Congressional action (Judicial Redress Act and USA Freedom Act)

Down to the Wire – Safe Harbor 2.0?

- Negotiations over how companies can transfer personal data across the Atlantic are ongoing, and a vote is expected by February 2nd.
- Two critical issues in negotiations. EU has asked for:
  - (1) Mandatory transparency reports from companies on national security orders.
  - (2) Expanded involvement of EU Data Protection Authorities jurisdictionally

Down to the Wire – Safe Harbor 2.0?

Several variables to look for in the next few days:

- EU reaction to new US proposals
- Increased pressure from companies to reach an agreement
- Judicial Redress Act
- Leeway on the deadline

What can US business expect with or without a Safe Harbor 2.0?

With a Safe Harbor Agreement?	Without a Safe Harbor Agreement?
- There will still be details to work out and DPAs will review new framework	- DPAs may extend the effective deadline for negotiations
- Business must meet new Safe Harbor requirements	- Business must rely solely on other methods of transfer
- Prepare for new claims by EU data subject and increased scrutiny generally	- Any data transfers may be challenged by EU data subject and digital-rights advocates

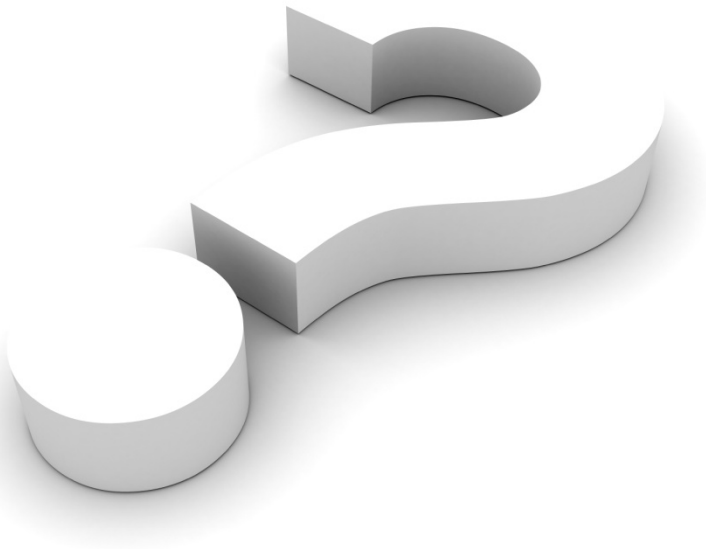
What can European businesses expect?

- Prospects for extension of the timetable for implementation of safe harbor 2.0
- What transfers are open to challenge and who will challenge them?
- What will happen to standard contractual terms

How your organisation should react to this decision

- If your organisation or its service providers are Safe Harbor certified:
  - Conduct an urgent review to identify the types of personal data being transferred and processed and the purposes for which that personal data are being transferred and processed under Safe Harbor;
  - Determine if that personal data is being transferred under any other mechanisms that have been determined to be adequate in addition to Safe Harbor (e.g. the standard contractual clauses, binding corporate rules etc);
  - Where Safe Harbor alone is being relied upon to transfer that data, determine if it is possible to suspend processing of personal data under Safe Harbor or conduct it in the EU until alternative mechanisms for processing such personal data can be put in place; and
  - Put in place alternative mechanisms for transferring that personal data to the US as soon as possible and in any event before 31 January 2016.

Questions



Mark Prinsley
Partner - London
+44 203 130 3900
mprinsley@mayerbrown.com

Kendall Burman
Counsel – Washington DC
+1 (202) 263 3210
kburman@mayerbrown.com

Oliver Yaros
Senior Associate - London
+44 203 130 3698
oyaros@mayerbrown.com