This Webcast Will Begin Shortly

If you have any technical problems with the Webcast or the streaming audio, please contact us via email at:

webcast@acc.com

Thank You!
ACC Webinar - does the US-EU Privacy Shield solve your global Data Concerns?

Nick Holland, Partner, Fieldfisher
1 December 2016
101 on EU data export rules

- EU has strictest privacy regime in the world
- Prohibition on international data flows, unless...
  - ... have in place 'adequate' protection
- Very limited, narrowly interpreted restrictions
- Serious impairment to global business
101 on EU data export rules

- Article 25 of the Data Protection Directive (95/46/EC):

1. The Member States shall provide that the transfer to a third country of personal data … may take place only if … the third country in question ensures an **adequate** level of protection.

6. The Commission may find … that a third country ensures an **adequate** level of protection … by reason of its domestic law or of the international commitments it has entered into … for the protection of the private lives and basic freedoms and rights of individuals.
What are your options?

**Exceptions (Art 26(1))**
- Unambiguous consent?
- Contractual necessity?
  - Vital interests?
  - Public interest?
  - Legal claims?

**Compliance Solutions**
- Model clauses?
- Safe Harbor/Privacy Shield?
- Global DTA?
- Binding Corporate rules?
Why not just rely on consent or contractual necessity?

The Article 29 Working Party recommends that the derogations in Article 26(1) of the Directive should be interpreted restrictively ... 

This is the case in particular for transfers of personal data that might be described as repeated, mass or structural. These transfers should, where possible, and precisely because of their importance, be carried out within a specific legal framework (Article 25 or 26(2)). Only for instance when recourse to such a legal framework is impossible in practice can these mass or repeated transfers be legitimately carried out on the basis of Article 26(1).

Source: DG Justice, European Commission: Frequently Asked Questions relating to transfers of personal data from the EU/EEA to third countries
http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf
What are your options?

Exceptions (Art 26(1))
- Unambiguous consent?
- Contractual necessity?
- Vital interests?
- Public interest?
- Legal claims?

Compliance Solutions
- Model clauses?
- Safe Harbor/Privacy Shield?
- Global DTA?
- Binding Corporate rules?
PART I:
THE PROBLEM WITH MODEL CLAUSES
Everything you need to know about Model Clauses

- Data export contract, blessed by the European Commission
- Bipartite – envisage a one-to-one relationship, not one-to-many
- 3 flavours exist – make sure to use the right one!
  - Controller-to-Controller (2001) – NEVER, EVER USE!
  - Controller-to-Processor (2010) – CUSTOMER TO SERVICE PROVIDER TRANSERS
- Beloved by EU controllers – terms very much in their favour!
- Enable transfers from exporting EU controller to importing entities anywhere in the world
- The solution of choice for EU regulators
# Model Clauses – pros and cons

<table>
<thead>
<tr>
<th><strong>Pros</strong></th>
<th><strong>Cons</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A ‘guaranteed compliant’ solution</td>
<td>An administrative nightmare for large transfers!</td>
</tr>
<tr>
<td>Controller and processor versions exist</td>
<td>Wholly uncommercial terms</td>
</tr>
<tr>
<td>Relatively quick to execute</td>
<td>No real ability to amend</td>
</tr>
<tr>
<td>Enable worldwide exports (not just US)</td>
<td>No limitation on liability</td>
</tr>
<tr>
<td>Never enforced (yet)</td>
<td>Subcontracting restrictions</td>
</tr>
<tr>
<td>Your EU customers will like it</td>
<td>Audit rights</td>
</tr>
<tr>
<td></td>
<td>Do little for privacy in practice</td>
</tr>
<tr>
<td></td>
<td>Need many hundreds of them for global transfers</td>
</tr>
<tr>
<td></td>
<td>Still have to file them with DPA’s</td>
</tr>
</tbody>
</table>
What are your options?

**Exceptions (Art 26(1))**
- Unambiguous consent?
- Contractual necessity?
- Vital interests?
- Public interest?
- Legal claims?

**Compliance Solutions**
- Model clauses?
- Safe Harbor/Privacy Shield?
- Global DTA?
- Binding Corporate rules?
PART II:
THE PROBLEM WITH SAFE HARBOR
Safe Harbor Under Siege

- **June 2010:** Düsseldorfer Kreis resolution for German companies relying on Safe Harbor.

- **June 2013:** Snowden revelations about NSA mass surveillance.

- **November 2013:** EU Commission issues “Communication” to the European Parliament and the Council. 13 recommendations for improvement.

- **March 2014:** EU Parliament votes to suspend Safe Harbor (but not their competence to suspend).

- **June 2014:** Schrems v Irish DPC before Irish courts.

- **February 2015:** Two German authorities (Berlin and Bremen) take action against two US Safe Harbor companies.

- **March 2015:** Schrems v Irish DPC goes to the ECJ. Safe Harbor put in the dock.

- **6 Oct 2015:** ECJ’s Schrems decision declares Safe Harbor invalid
Enter the EU – US Privacy Shield

- **16 Oct 2015**: A29 WP gives EU-US authorities until end of January 2016 to find a workable solution.
- **28 Jan 2016**: Amendment to Judicial Redress Act disrupts and delay negotiations on new framework.
- **2 Feb 2016**: 11th hour agreement reached. EC issues press release – re: agreement on data flows
- **29 Feb 2016**: EU Commission has publishes the Privacy Shield docs and a draft adequacy decision
- **16 March 2016**: 27 civil rights organizations say draft Privacy Shield not good enough.
- **13 April 2016**: A29 WP publishes (negative) opinion on the Privacy Shield draft adequacy decision.
- **26 May 2016**: EU Parliament calls on Commission to re-open negotiations with US on the Privacy Shield
- **8 July 2016**: A31 Committee (representatives of Member States) approve final version of Privacy Shield.
- **12 July 2016**: Commission formally adopts Privacy Shield Framework.
- **26 July 2016**: A29 WP press statement
- **1 August 2016**: EU Privacy Shield commenced
Privacy Shield: Safe Harbor on steroids?

Requirements that are reinforced under Privacy Shield

• Applies to transfers from both controllers and processors (agents)
• 7 Privacy Shield Principles: impose stricter and more comprehensive data protection obligations on U.S. organizations that handle EU personal data.
• Transparency and administration by DoC reinforced:
  – DoC must make publicly available list of self-certified companies (Privacy Shield List) + update this list annually
  – DoC must keep a record of companies that have been removed from this List and why
  – DoC must provide link to Privacy-Shield related FTC enforcement cases on FTC’s website
• Oversight and verification of compliance by DoC reinforced:
  – Privacy policies comply to the Principles;
  – Personal data returned, deleted or retained in accordance with Principles if company no longer member of Privacy Shield
  – Monitoring of websites for false claims and misrepresentations
  – Ex officio compliance reviews of self-certified organisations
  – Possibility to remove a company from the Privacy Shield in case of a failure to comply
Privacy Shield Redress Mechanisms

Individuals have access to multiple redress mechanisms:

• Complaint to the **self-certified organisation** (response within 45 days)
• **Independent dispute resolution body** (either in the U.S. or the EU) designated by the organisation itself
• **National Data Protection Authority**: organization must cooperate with DPA when it has voluntarily submitted to the oversight by DPA or when the processing concerns employee data.
• **Department of Commerce**: complaint made directly to a DPA and then channelled to DoC via a dedicated contact point
• **Federal Trade Commission**: accepts complaints directly from individuals
• **Privacy Shield Panel**: pool of 20 arbitrators designated by the DoC and the EU Commission + arbitration decision is enforceable in the U.S. courts under the Federal Arbitration Act.
Privacy Shield: going beyond Safe Harbor

New elements under the Privacy Shield
• Voluntary withdrawal from Privacy Shield
• Privacy Shield Panel
• Limitations on access and use of personal data by U.S. public authorities
• Privacy Shield Ombudsperson
• Annual joint review mechanism
• Role of the national DPAs
• Suspension, amendment or repeal of the EU Commission’s adequacy decision
Part 4:
Is the Privacy Shield right for your organisation?
• Privacy Shield: What does it do for me?
Privacy Shield: Is it any good?

The European Commission should hold off on activating Privacy Shield until more work is done on the US side. Given the countless insufficiencies, it is otherwise highly likely that the new Privacy Shield will share the history of the previous Safe Harbor and be invalidated by the European Court of Justice.

We have agreed on a new strong framework on data flows with the US. Our people can be sure that their personal data is fully protected. Our businesses, especially the smallest ones, have the legal certainty they need to develop their activities across the Atlantic.

Jan-Philipp Albrecht, German MEP

Commission Vice-President Andrus Ansip
<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The <strong>only</strong> available compliance solution for some companies</td>
<td>• A lot of uncertainty still – virtually guaranteed to be challenged</td>
</tr>
<tr>
<td>• Competitors will adopt it – and you need to keep up with the Jones’s!</td>
<td>• Customers will still want you to sign model clauses with them</td>
</tr>
<tr>
<td>• (Mostly) enforced by a “known entity” regulator, not some unknown European DPA</td>
<td>• FTC will be under intense pressure to enforce non-compliance</td>
</tr>
<tr>
<td>• Self-certification highly preferable as compared with lengthy BCR approvals</td>
<td>• Joint annual review mechanism – unknown if and how the Shield will change with time</td>
</tr>
<tr>
<td>• No need for consent to appoint data processors, and no customer audit rights</td>
<td>• What is meant by “same level of protection” in the onward transfer mechanism</td>
</tr>
<tr>
<td>• 9 month “grace period” to sort out subcontractors for early registrants</td>
<td>• Still only a US-EU solution and <strong>not</strong> a global solution</td>
</tr>
<tr>
<td>• In time US “sales cachet”?</td>
<td>• Interplay between the Shield and Model Clauses very uncertain</td>
</tr>
</tbody>
</table>
Where the Shield works well (1)

Consumer Co, Inc.

US

EU

Personal data

Consumers

- Model Clauses
- Binding Corporate Rules
- Privacy Shield
Where the Shield works well (2)

Global Co, Inc.

- Model Clauses
- Binding Corporate Rules
- Privacy Shield

EU Sub 1 (controller)
EU Sub 2 (controller)
EU Sub 3 (controller)

Personal data (HR, CRM)
Where the Shield doesn’t work so well (1)

Global Co (US)

Non-EU Sub (India)

Model Clauses

Binding Corporate Rules

Privacy Shield

EU

Non-EU

EU Sub 1 (controller)

EU Sub 2 (controller)

EU Sub 3 (controller)

Personal data
Hi Mr. Supplier. I’d like you to process some data for me. But you’re in the US. **How will you comply with EU data export rules?**

Hi Ms. Customer. We’d love to. And don’t worry about EU data rules, we’re Privacy Shield certified!

I’ve heard of the Privacy Shield, but my DPO doesn’t trust it. He says it may be declared invalid, like Safe Harbor. **We’d like you to sign Model Clauses or have Processor BCR.**
EU-US Privacy Shield – pros and cons

• Fine if transferring to the US only – NOT suitable for global data transfers which is the case for most multinationals

• Depending on take up there may be a US sales cachet-early signs are that quite a few US companies have applied by Sept 30

• Annual review process – it may change how privacy shield works overtime

• A lot more scrutiny by the EU DPAs

• Significant exposure to FTC-more pressure on enforcement

• Is being challenged by Digital Rights Ireland and French privacy groups and no doubt others will follow
What are your options?

Exceptions (Art 26(1))

- Unambiguous consent?
- Contractual necessity?
- Vital interests?
- Public interest?
- Legal claims?

Compliance Solutions

- Model clauses?
- Safe Harbor/Privacy Shield?
- Global DTA?
- Binding Corporate rules?
PART III:
THE BUSINESS CASE FOR GLOBAL DTA
Global DPAs

- Is a global agreement signed by all internal entities
- Based on model clauses but modernised
- Map of data flows and systems needed
- Accession Schedule added to allow for growth or contraction of corporate structure
- Is a good solution where BCR is considered too expensive, will take too long and/or you need something in the meantime while you wait for BCR
Global DPAs – Pros and Cons

Pros:

• Reasonably quick to finalise (1-3 months)
• Deals with audits subcontracting rights and liability
• Allows for growth and contraction of corporate structures
• Shows to your employees and customers you have privacy and security protocols in place

Cons:

• Still need to file with DPAs
• Time is needed to map data flows
• Will not cover Germany as model clauses will still be required
PART IV:
THE BUSINESS CASE FOR BCR
What springs to mind when you think of BCR
EU Privacy Reform – the big picture

- Root and branch reform
- Applicable to controllers and processors
- Single, harmonized regime throughout Europe
- Extra-territorial effect
- Significant emphasis on accountability
- BCRs take centre-stage!
How BCR will help you

- BCR deliver a global (not just US) compliance framework and are recognized not just in Europe but also in other parts of the world (e.g., Australia, South Africa, Singapore)
- Accountability-based solution: many companies are effectively doing BCR but simply need to formalize it
- Reduce deal negotiation lag - customers will like BCR
- The only real data export solution available for data processors
- BCR flexibility facilitates global group-wide expansion
- Puts you at a competitive advantage and increases the trust of your customers
- Will be a key part of providing “accountability” under GDPR
BCR – pros and cons

**Pros**

- The ‘gold standard’ in the EU
- A solution for controllers and processors
- High degree of self-determination
- Good relationship-building with DPAs
- Provides an entire compliance framework
- Widely recognized in many non-EU territories
- Good for PR and sales
- High degree of future-proofing
- Provides GDPR accountability
- Accelerates and compliments GDPR compliance program

**Cons**

- Long lead time to implement – 12-18 months
- Experience very dependent on lead DPA but you have some flexibility to choose
- Heavier to implement but more effective for compliance
- Requires approval from three DPAs before mutual recognition process.
What do BCR comprise?

- BCR Policy
- Audit Protocol
- Complaint Handling Procedure
- Subject Access Request Procedure
- DPA Cooperation Procedure
- BCR Updating Procedure
- Training
- Binding Mechanism
What the process entails

DPA reviews comprise:
1. Initial review by the Lead authority
2. Co-review by two supporting DPAs
3. Mutual recognition peer review (other DPAs)
4. Cooperation procedure review (DPAs not under mutual recognition)
BCR – Sounds great, but who else has them?


<table>
<thead>
<tr>
<th>Company name</th>
<th>Lead authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABN AMRO Bank N.V.</td>
<td>Dutch DPA</td>
</tr>
<tr>
<td>Astra Zeneca plc</td>
<td>ICO (UK)</td>
</tr>
<tr>
<td>Accenture</td>
<td>ICO (UK)</td>
</tr>
<tr>
<td>Airbus (Controller)</td>
<td>CNIL (FR)</td>
</tr>
<tr>
<td>Akzo Nobel N.V. (Controller)</td>
<td>Dutch DPA</td>
</tr>
<tr>
<td>Align Technologies B.V. (Controller)</td>
<td>Dutch DPA</td>
</tr>
<tr>
<td>American Express</td>
<td>ICO (UK)</td>
</tr>
<tr>
<td>ArcelorMittal Group</td>
<td>Luxemburg</td>
</tr>
<tr>
<td>Atmel</td>
<td>ICO (UK)</td>
</tr>
<tr>
<td>Atos (Controller and Processor)</td>
<td>CNIL (FR)</td>
</tr>
<tr>
<td>AXA</td>
<td>CNIL (FR)</td>
</tr>
<tr>
<td>Axa Private Equity</td>
<td>CNIL (FR)</td>
</tr>
</tbody>
</table>
Conclusions

- EU Privacy Shield is more effective than safe harbor
- It will no doubt attract sales cachet for US customers
- On its own it will not be enough for global compliance
- For any company which has lots of data, dealing with customer issues with data or sees it as a competitive sales advantage, BCR is the way forward
- BCR will significantly help with GDPR compliance
- If you apply for BCR in the next few months likely to have it in place by May 2018
- Fieldfisher have led on 20% of all BCR’s approved
Questions?

Nick Holland
Partner - London
Fieldfisher

E: nick.holland@fieldfisher.com
T: +44 (0)20 7861 4977
M: +44 (0) 7774 975559
Thank you for attending another presentation from ACC’s Webcasts

Please be sure to complete the evaluation form for this program as your comments and ideas are helpful in planning future programs.
If you have questions about this or future webcasts, please contact ACC at webcast@acc.com

This and other ACC webcasts have been recorded and are available, for one year after the presentation date, as archived webcasts at http://www.acc.com/webcasts