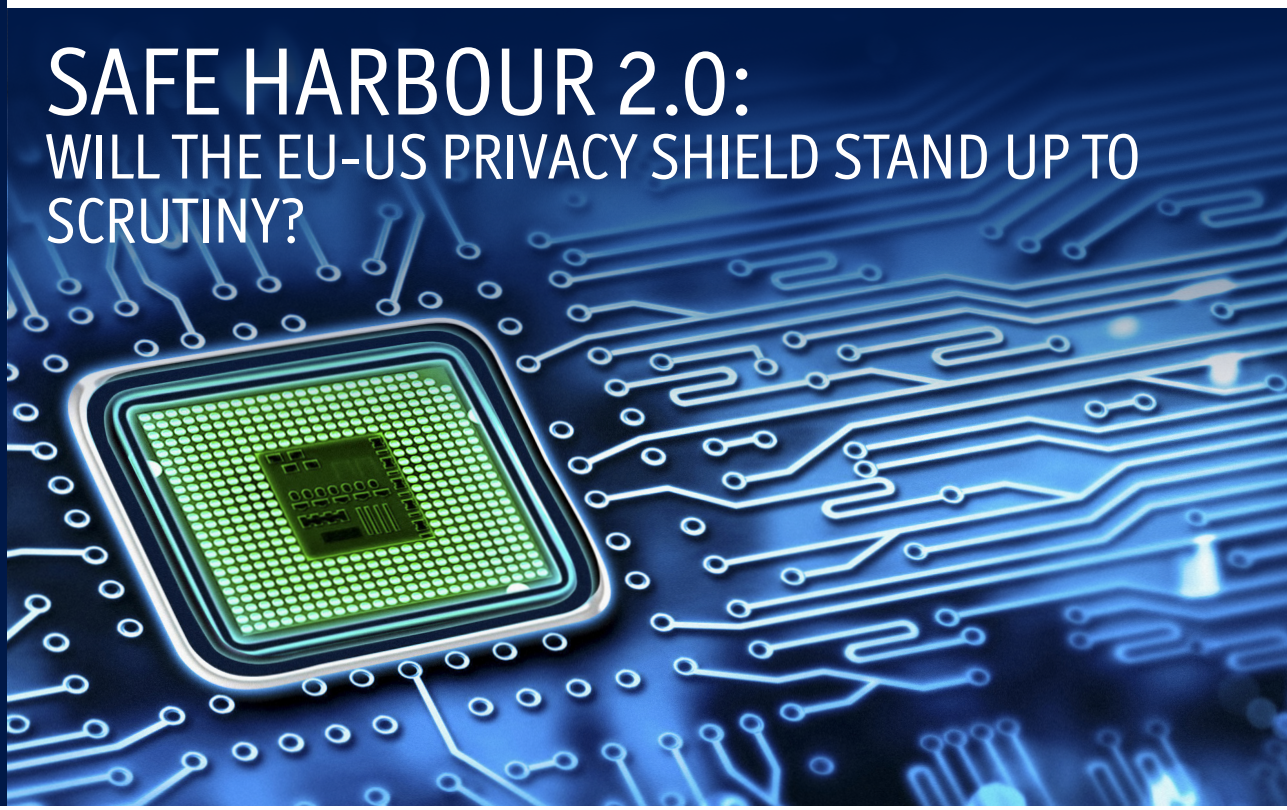
EU, Competition and Regulatory

February 2016

SAFE HARBOUR 2.0:
WILL THE EU-US PRIVACY SHIELD STAND UP TO SCRUTINY?



A last minute deal was struck on 2 February 2016 between the European Commission and the United States, in an attempt to fill the void in EU-US data transfer created by the Schrems[1] decision in October 2015. The political agreement creates a new framework for transatlantic data flows, labelled the "EU-US Privacy Shield". The name implies robust protection for EU citizens' data, but the level of protection offered by the framework is already being called into question by critics across Europe.

The new deal

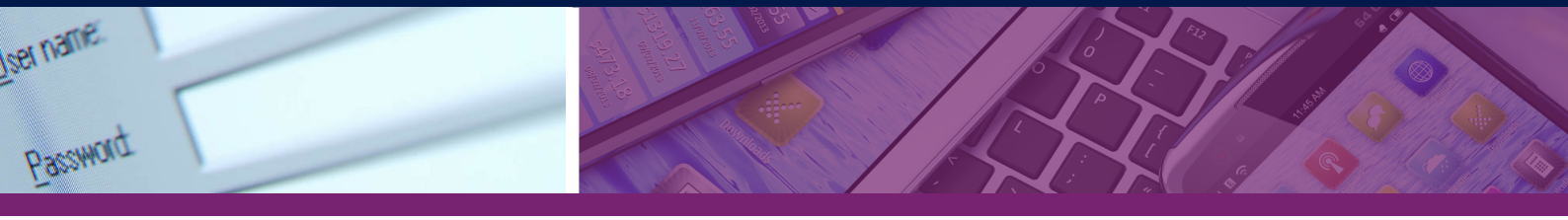
The new arrangement is said to include the following elements[2]:

1. **Strong obligations on companies handling Europeans' personal data and robust enforcement**
   As with the original Safe Harbour framework, US companies wishing to import personal data from Europe will need to commit to obligations on how personal data is processed and individual rights are guaranteed. The new EU-US Privacy Shield is intended to make these obligations more robust. The US Department of Commerce will monitor that companies publish their commitments, which makes them enforceable under US law by the US Federal Trade Commission (FTC). Any company handling human resources data from Europe must commit to comply with decisions by European DPAs.

2. **Clear safeguards and transparency obligations on US government access**
   The US has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. Access must be only to the extent that it is necessary and proportionate. Surveillance on personal data transferred to the US under the new arrangement will no longer be 'indiscriminate

1 Case C-362/14 (Schrems) – 6 October 2015, see http://curia.europa.eu/juris/liste.jsf?num=C-362/14

2 See the European Commission's press release of 2 February 2016: http://europa.eu/rapid/press-release_IP-16-216_en.htm



mass surveillance'. An annual joint review by the European Commission and the US Department of Commerce will monitor the functioning of the arrangement. This review will include the issue of national security access. The European Commission and the US Department of Commerce will invite national intelligence experts from the US and European Data Protection Authorities to join the review.

3. **Effective protection of EU citizens' rights with several redress possibilities**
   Any citizen who considers that their data has been misused under the new arrangement will have a number of options for redress. Companies will have deadlines to reply to complaints. Individuals will be encouraged to complain to their national European DPAs, which can refer complaints to the US Department of Commerce and the US Federal Trade Commission. Participation in alternative dispute resolution will be incorporated into US companies' obligations, free of charge to data subjects. A new ombudsperson will be created to address complaints on possible access by national intelligence authorities.

The European Commission aims to prepare a draft 'adequacy decision' within the next few weeks. This is subject to the advice of the Article 29 Working Party (A29WP), composed of representatives from each Member State's Data Protection Authority.

Article 29 Working Party

So far, the new deal does not seem to have convinced the A29WP, at least according to its statement of 3 February 2016[3]. In its statement, the A29WP expressed *"concerns on the current US legal framework as regards the four essential guarantees, especially regarding scope and remedies".*

The A29WP considered European jurisprudence, which sets four essential guarantees for intelligence activities:

"A. Processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;

B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual;

C. An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;

D. Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body."

A29WP intends to hold an extraordinary meeting at the end of March or early April to decide whether to endorse the EU-US Privacy Shield. A29WP will also decide at its extraordinary meeting whether Standard Contractual Clauses (Model Clauses) and Binding Corporate Rules (BCRs) will provide sufficient protection to allow transfer of EU personal data to the US.

Does the EU-US Privacy Shield plug the Safe Harbour gaps?

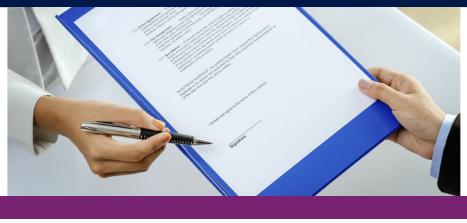
The first Safe Harbour framework was struck down in *Schrems* for a number of reasons. Key factors were that:

- The level of US intelligence services' surveillance of personal data collected under the framework, as revealed by Edward Snowden in 2013, was inherently disproportionate.
- EU citizens do not have the same right to redress in the US as they do in the EU.

These points have been made by European commentators for some time. A 'Safe Harbour 2.0' has been in the works for years, but it took the Schrems ruling, and the A29WP reaction to it, to put the requisite pressure on the US and EU negotiators to reach a new deal.

Efforts have clearly been made to address the issues of over-invasive surveillance and a lack of redress for EU citizens, and to increase enforcement and cross-border cooperation. However, judging by the less than enthusiastic statement from the A29WP on 3 February, these may well not be enough.

3 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf


What should businesses do now?

Current advice from the A29WP and the US FTC is that businesses should continue to use the Model Clauses, BCRs and the derogations listed in letters (a) to (f) of Article 26(1) of Directive 95/46/EC[4] to transfer data to the US. The derogations include:

The data subject has unambiguously given his/her consent to the proposed transfer.

- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject.
- The transfer is made from a public register.

It should be noted that the derogations will be applied very strictly, and businesses should ideally take legal advice before seeking to rely on a particular derogation. The A29WP has issued a number of 'best practice' rules, and recommends that 'repeated, mass or structural' transfers of personal data should, where possible, be carried out using the Model Clauses or BCRs[5].

Efforts have clearly been made to address the issues of over-invasive surveillance and a lack of redress for EU citizens, and to increase enforcement and cross-border cooperation. However, judging by the less than enthusiastic statement from the A29WP on 3 February, these may well not be enough.

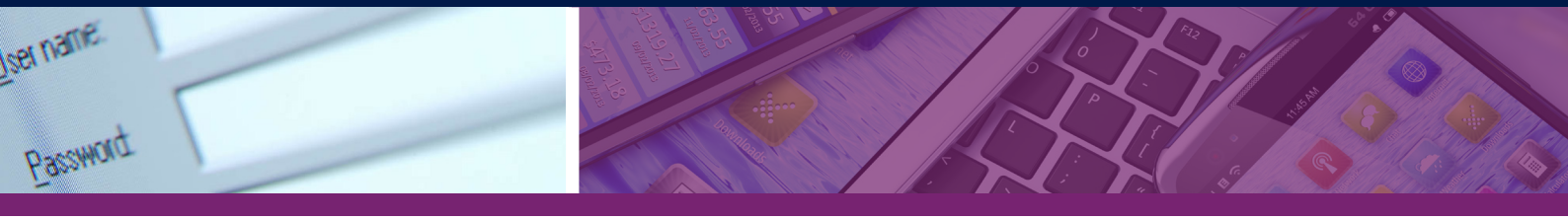
FELICITY BURLING, ASSOCIATE

BCRs are not ideal at present because these can take well over a year to orchestrate, and some national DPAs are currently reluctant to approve data transfer contracts or BCRs involving transfer to the US. The German DPAs, for example, are refusing to approve any new BCRs for transfer of personal data to the US until the issue of US adequacy has been resolved.

Model Clauses, for the moment, and the cautious use of the derogations in letters (a) to (f) of Article 26(1) of Directive 95/46/EC, remain the safest options.

4 For Commission guidance on the use of alternative transfer mechanisms for transfer of personal data from the EU to the US, see http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

5 See A29WP opinion of 25 November 2005: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf



For more information, please contact the authors of this briefing:

Anthony Woolich
Partner, London
T: +44 (0)20 7264 8033
E: anthony.woolich@hfw.com

Felicity Burling
Associate, London
T: +44 (0)20 7264 8057
E: felicity.burling@hfw.com

HFW has over 450 lawyers working in offices across Australia, Asia, the Middle East, Europe and South America. For further information about EU, Competition and Regulatory issues in other jurisdictions, please contact:

Daniel Martin
Partner, London
T: +44 (0)20 7264 8136
E: daniel.martin@hfw.com

Robert Follie
Partner, Paris
T: +33 1 44 94 40 50
E: robert.follie@hfw.com

Pierre Frühling
Partner, Brussels
T: +32 (0) 2643 3406
E: pierre.fruhling@hfw.com

Jeremy Davies
Partner, Geneva
T: +41 (0)22 322 4810
E: jeremy.davies@hfw.com

Jasel Chauhan
Partner, Piraeus
T: +30 210 429 3978
E: jasel.chauhan@hfw.com

Ian Chung
Partner, Dubai
T: +971 4 423 0534
E: ian.chung@hfw.com

Brian Gordon
Partner, Singapore
T: +65 6411 5333
E: brian.gordon@hfw.com

Guy Hardaker
Partner, Hong Kong
T: +852 3983 7644
E: guy.hardaker@hfw.com

Julian Davies
Partner, Shanghai
T: +86 21 2080 1188
E: julian.davies@hfw.com

Aaron Jordan
Partner, Melbourne
T: +61 (0)3 8601 4535
E: aaron.jordan@hfw.com

Stephen Thompson
Partner, Sydney
T: +61 (0)2 9320 4646
E: stephen.thompson@hfw.com

Simon Adams
Partner, Perth
T: +61 (0) 8 9422 4715
E: simon.adams@hfw.com

Fernando Albino
Partner, São Paulo
T: +55 (11) 3179 2900
E: fernando.albino@hfw.com

Lawyers for international commerce hfw.com

São Paulo London Paris Brussels Geneva Piraeus Beirut Riyadh Kuwait Abu Dhabi Dubai Singapore Hong Kong Shanghai Perth Melbourne Sydney