

EU-US Privacy Shield in force

On 12 July 2016 the European Commission adopted the final version of the EU-U.S. Privacy Shield, which enables the transfer of personal data between the EU and the U.S. The Privacy Shield replaces the Safe Harbor arrangement, which was invalidated by the European Court of Justice in October 2015 (see our previous briefings).

Valid legal basis for data transfer to the US

The European Commission has adopted the Privacy Shield pursuant to a so-called "adequacy decision", through which it can allow the transfer of personal data to a country outside the European Economic Area (EEA) on the basis that the recipient country ensures an adequate level of protection for the transferred data.

The U.S. will be regarded as providing an adequate level of protection for personal data transferred to companies that comply with the requirements of the Privacy Shield – such transfers will therefore not breach EU restrictions on the international transfer of personal data. The Privacy Shield does not apply to data transfers to jurisdictions other than the U.S., nor to transfers to U.S. companies who do not participate in the Privacy Shield. Participation is only available to U.S. companies that are regulated by the U.S. Federal Trade Commission or Department of Transportation and is not, therefore, available to (for example) financial institutions. It is likely, however, that many other U.S. companies, and particularly many IT companies providing services to customers within the EEA, will participate.

Privacy Shield

The Privacy Shield consists of Privacy Principles that companies must abide by and commitments by the U.S. government on how the arrangement will be enforced and more widely on the exercise of its own risks of access to personal data transferred from the EEA. The arrangement imposes strong obligations for companies in the U.S. handling data from the EEA, including strict conditions for onward transfers. U.S. companies will be subject to oversight mechanisms to ensure compliance. There are safeguards and transparency obligations regarding U.S. government access, including written assurance from the

U.S. government that data access by its agencies will be subject to defined limitations. European citizens who consider that their data have been misused will have several redress possibilities. The functioning of the Privacy Shield and U.S. commitments will be reviewed annually, so that the European Commission can take appropriate measures to continue ensuring an adequate level of protection.

How does it work?

Like the former Safe Harbor framework, the Privacy Shield is based on self-certification. As part of this certification, companies in the U.S. must commit to the Privacy Principles. Compliance with the Privacy Principles entails, amongst other things that U.S. companies will need to comply with information and purpose limitation requirements, take security measures and grant individuals access rights to their data. Companies must also make their privacy policies public and provide links to (i) the website of the U.S. Department of Commerce, (ii) the Privacy Shield List, and (iii) the website of an appropriate alternative dispute settlement provider. Each certification must be renewed annually. The U.S. Department of Commerce will maintain the public Privacy Shield List of participating companies.

Conclusion

The Privacy Shield entered into force on 12 July 2016. US companies will have the opportunity to certify compliance with the Privacy Principles with the U.S. Department of Commerce from 1 August 2016. In parallel, the Commission will publish a short guide for citizens, explaining the available remedies in case an individual considers that his or her personal data has been used without taking into account the data protection rules.

The Privacy Shield still faces criticism from privacy activists on the basis that it does not adequately protect EU personal data from U.S. governmental access and further legal challenge may follow. One of the alternatives is to use the standard EU Model Contracts for the transfer of personal data outside the EEA, including to the U.S., although these are also subject to challenge, in a case that has already been referred to the EU Court of Justice. For now, the Privacy Shield is a valid legal basis for data transfers to the U.S. Companies with U.S. operations that are eligible to join may therefore wish to consider joining. Furthermore, if you use or are looking to use U.S. service providers who process personal data on your behalf, consider discussing with them whether they plan to self-certify to the Privacy Shield – for the time being, at least, it may be more secure than the EU Model Contracts as a mechanism for justifying transfer of personal data to the U.S., and it also has the advantage that it does not require prior approval of a data protection authority in any EEA member state, while several member states still only recognise the Model Contracts based on pre-approval.

For any assistance with self-certifying to the Privacy Principles, please contact Megan Gordon or Steven Gatti or your regular Clifford Chance contact. For assistance regarding EU restrictions on international transfer of personal data, please contact Nadia Jagusiak, Richard Jones, Jonathan Kewley or, again, your regular Clifford Chance contact.

Contacts

Steven Gatti

T: +1 20 2912 5095

E: [steven.gatti](mailto:steven.gatti@cliffordchance.com)

[@cliffordchance.com](https://www.instagram.com/cliffordchance.com)

Megan Gordon

T: +1 20 2912 5021

E: [megan.gordon](mailto:megan.gordon@cliffordchance.com)

[@cliffordchance.com](https://www.instagram.com/cliffordchance.com)

Nadia Jagusiak

T: +31 20 711 9210

E: [nadia.jagusiak](mailto:nadia.jagusiak@cliffordchance.com)

[@cliffordchance.com](https://www.instagram.com/cliffordchance.com)

Richard Jones

T: +44 20 7006 8238

E: [richard.jones](mailto:richard.jones@cliffordchance.com)

[@cliffordchance.com](https://www.instagram.com/cliffordchance.com)

Jonathan Kewley

T: +44 20 7006 3629

E: [jonathan.kewley](mailto:jonathan.kewley@cliffordchance.com)

[@cliffordchance.com](https://www.instagram.com/cliffordchance.com)

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, Droogbak 1A, 1013 GE Amsterdam, PO Box 251, 1000 AG Amsterdam

© Clifford Chance 2016

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571. Registered office: 10 Upper Bank Street, London, E14 5JJ. We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications. Clifford Chance LLP is registered in the Netherlands with the commercial register of the Chamber of Commerce under number 34360401. For our (notarial) third party account details, please see www.cliffordchance.com/nlregulatory

Abu Dhabi ■ Amsterdam ■ Bangkok ■ Barcelona ■ Beijing ■ Brussels ■ Bucharest ■ Casablanca ■ Doha ■ Dubai ■ Düsseldorf ■ Frankfurt ■ Hong Kong ■ Istanbul ■ Jakarta* ■ London ■ Luxembourg ■ Madrid ■ Milan ■ Moscow ■ Munich ■ New York ■ Paris ■ Perth ■ Prague ■ Riyadh ■ Rome ■ São Paulo ■ Seoul ■ Shanghai ■ Singapore ■ Sydney ■ Tokyo ■ Warsaw ■ Washington, D.C.

*Linda Widyati & Partners in association with Clifford Chance.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.