ESPC

Email Sender & Provider Coalition

Status of the Privacy Shield: What You Need to Know

Rosemary Smith

OPT-4

Data Protection Network

In 2004 Rosemary set up Opt-4 in which advises organisations on UK and international data protection compliance and the maximization of marketing permissions.

She has chaired the UK Direct Marketing and is a tutor for the Institute of Direct Marketing where she is currently delivering regular courses for marketers covering the impact of the new Data Protection Regulation.

Rosemary is a founder of the Data Protection Network a resource website for all those interested in data protection compliance.

https://www.dpnetwork.org.uk/

We'll cover

- Progress towards approval of the Privacy Shield
- How will it work?
- How will Privacy Shield commitments will be enforced?
- Arguments for and against
- Will it be approved by the European Commission and withstand scrutiny by the European Court of Justice?
- Alternatives to Privacy Shield
- Should you join Privacy Shield?

Data Protection Network

The story so far

- October 2015 – Safe Harbor struck down by European Court of Justice
- February 2016 – European Commission and US Department of Commerce presents Privacy Shield as solution
- April 2016 – Article 29 Working Party criticizes Privacy Shield
- June 2016 – Proposed adoption date?

Data Protection Network

How will it work?

Self certification with Department of Commerce
Agree to key principles

- Notice - Must inform individuals about the Privacy Shield, their rights, contact for complaints, details of sharing and disclosure of data (including disclosure to agencies such as the NSA) and the organisation's liability for data processing

- Choice - Individuals will have to be given the choice to opt-out, or to opt-in, as far as sensitive data is concerned, in relation to the disclosure of their data to a third party for marketing purposes or for any new use of their data which was not initially contemplated

- Accountability for onward transfer – Companies must put in place written contracts for transfers of data to other controllers or agents (data processors), subject to exceptions such as the occasional travel bookings for employees

Data Protection Network

How will it work?

- Security - Reasonable security measures which are appropriate taking into account the nature of the proposed processing and the personal data must be in place
- Data integrity and purpose limitation - Data collection has to be limited to what is relevant and data has to be kept accurate, complete, current and reliable
- Access - Individuals may access their data and arrange correction or deletion unless this would create a disproportionate burden or cost
- Recourse, enforcement and liability – Agree to the jurisdiction of Ombudsperson and a panel of representatives from European data protection authorities

Data Protection Network

Enforcement

- 45 days to deal with direct complaints
- Offer of independent recourse
- Referrals to DOC from local DPAs
- FTC to liaise with DPAs regarding enforcement
- Co-operation with Ombudsperson and DPA panel

"Strong law enforcement and increased cooperation will be critical to the new framework's success, and the FTC will play a significant role in enforcing commercial privacy promises under the framework."

Federal Trade Commission Chairwoman Edith Ramirez

Data Protection Network

Practical implications

- Public disclosure of privacy practices
- Additional compliance burden for company and sub-processors
- Potential for competitive advantage
- Provide choice /obtain consent from individuals

- Assess need for additional security
- Limit purposes of processing
- Institute dispute resolution processes
- Ensure access to data can be provided for individuals

Data Protection Network

The “pro” camp

Commissioner Jourová

"Protecting personal data is my priority both inside the EU and internationally. The EU-U.S. Privacy Shield is a strong new framework, based on robust enforcement and monitoring, easier redress for individuals and, for the first time, written assurance from our U.S. partners on the limitations and safeguards regarding access to data by public authorities on national security grounds.”

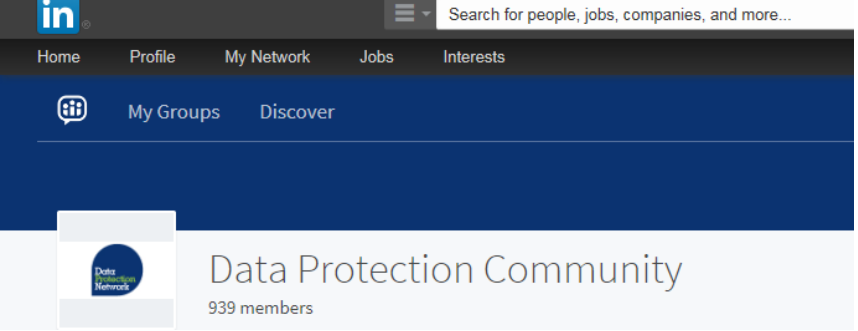
Data Protection Network

The “pro” camp

“The Privacy Shield strengthens cooperation between the Federal Trade Commission and EU Data Protection Authorities, providing independent, vigorous enforcement of the data protection requirements set forth in the Privacy Shield.

EU individuals will have access to multiple avenues to resolve concerns, including through alternative dispute resolution, now at no cost to the individual.”

Data Protection Network



"Ten layers of lipstick on a pig" Schrems verdict on the Privacy Shield

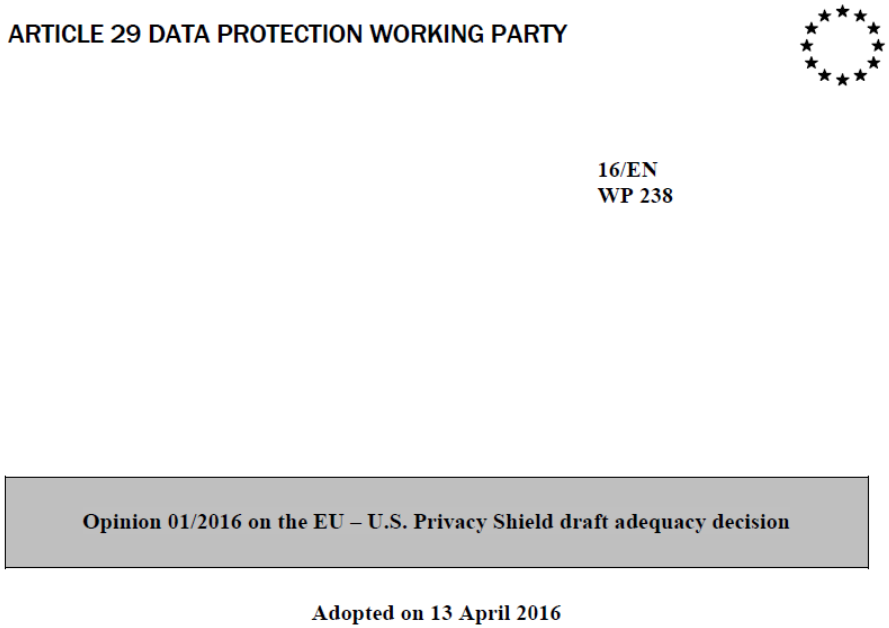
Max Schrems, whose action took down Safe Harbor, has expressed an opinion on the new Privacy Shield "They put ten layers of lipstick on a pig but I doubt the Court + DPAs suddenly want to cuddle with it" @maxschrems

Like Comment | 6

Data Protection Network

DPAs express “Strong concerns”

- Too many exemptions for law enforcement
- Ombudsperson not independent or powerful enough
- Principles fall short of European standards (e.g. retention)
- Lack of clarity on processor liabilities



ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 238

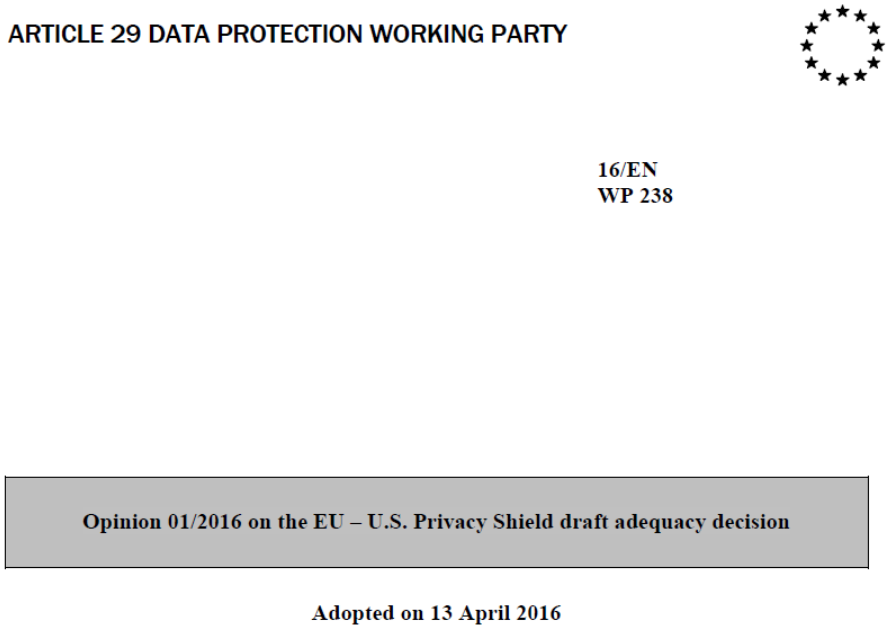
Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision

Adopted on 13 April 2016

Data Protection Network

DPAs express “Strong concerns”

- Exemptions too broad(journalism and public domain data)
- Doesn’t match forthcoming GDPR
- Remedies too complicated



ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 238

Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision

Adopted on 13 April 2016

UK Regulator view

Christopher Graham, the UK Information Commissioner

"If the data protection authorities, which are fairly expert in this area, are asking questions, then you can be pretty sure the European Court of Justice will also be asking questions. So it would be very sensible if both the EU and the US actually answered the questions.

"If there aren't answers there is only going to be trouble down the road. I would urge US corporates, which have a great interest in getting this sorted out, to encourage the US authorities to get answers to those questions so we can all move on safely,"

Data Protection Network

Will it be approved by the European Commission?

- Vera Jourova “the Commission will work to swiftly include [the Art 29 W/P concerns]in its final decision”
- European Commission may still adopt because of political and commercial pressures (possibly Sept)
- Likely Privacy Shield will be quickly challenged by DPAs and the Courts

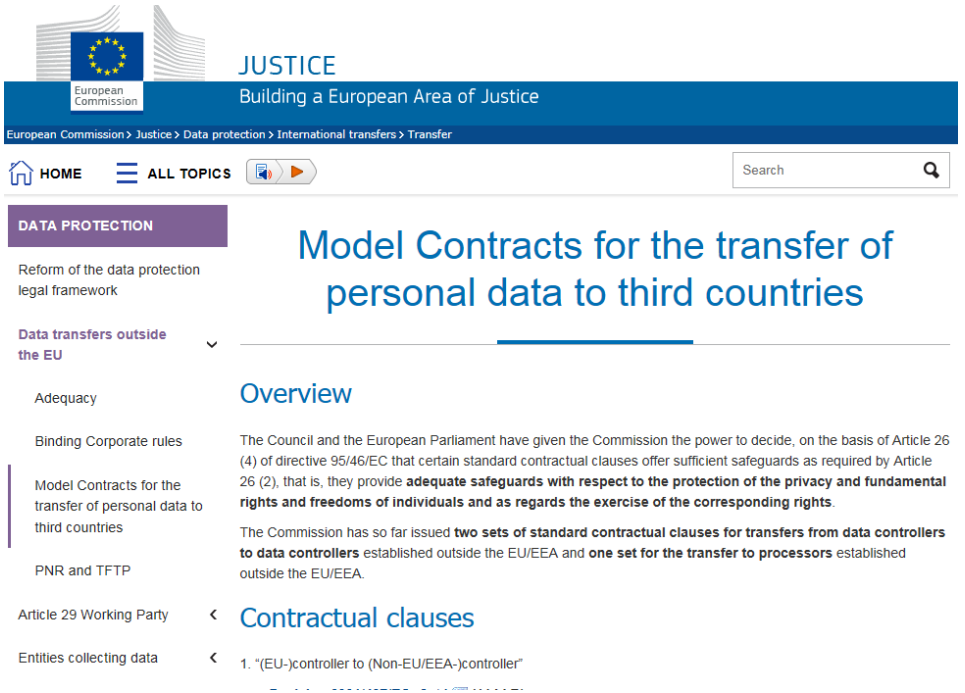
“Unfortunately, the legal uncertainty that many organisation face for the transfer of data to the US will remain for quite some time.”

Data Protection Network

Alternatives to Privacy Shield

- Binding Corporate Rules and Model Contracts both subject to future comment from Article 29 Working Party but valid at the moment

- Transfers based on Self Assessment of risk are possible (UK only and not after GDPR)



Should you join Privacy Shield?

- Only when it has been fully adopted
- Consider benefit/burden balance of joining
- Evaluate changes to data processing practices which will be needed
- Be aware of the risk that Privacy Shield will be struck down by the Courts

Data Protection Network