ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU-US Privacy Shield put into practice – first experiences

Some 200 companies had been certified towards the end of September. **Axel Spies** discusses the challenges already encountered and also what lies ahead of us.

The US Department of Commerce launched its self-certification system of the Privacy Shield (PS) on 1 August. The Commerce Department's PS website[1] provides information and assistance for US and European companies. Whoever expected long lines of registrants in front of the Department of Commerce building may be disappointed. Despite the publicity and huge expectations particularly in Europe, the enthusiasm among US companies has been lackluster. After

Continued on p.3

Privacy issues on the radar of competition authorities

How can regulators empower consumers and fight unfair user terms when they review mergers? **Laura Linkomies** reports from Brussels on the EU's Big Data challenge.

The EU Google antitrust case in 2014 set the alarm bells ringing: as Google has 90% of the European search market, has it abused its position? The answer from the European Commission was no, but Google had to make some concessions. In 2015, Disconnect, a US firm that designs privacy-enhancing technologies, filed a complaint against Google for violating privacy rights – Disconnect argued that

Continued on p.6

Issue 143 **October 2016**

INTERNATIONAL report

ISSUE NO 143 OCTOBER 2016

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

SUB EDITOR
Tom Cooper

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Axel Spies
Morgan Lewis LLP, US

Anna Romanou
Eurofins, Belgium

Stefania Tonutti
PhD in Law and New Technologies, Italy

Scott Livingston
SIPS Asia, Hong Kong

Philip Woolfson and Daniella Terruso
Steptoe & Johnson LLP, Belgium

Rena Mears, Ryan Sulkin, Eric Roth and Jim Halpert,
DLA Piper LLP, US

Merrill Dresner
PL&B Correspondent

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

World of privacy shrinks as we share the same issues

Large mergers affect not only people as workers or consumers but also in terms of privacy protection – read on p.1 what the European Data Protection Supervisor and BEUC, the European Consumer Organisation, are trying to do about it. Data localisation laws, the requirement to process personal data in a country, are becoming better known now. It is not only an issue in Russia, but also in China and to some extent, also in some other APEC countries (p.22).

EU-US Privacy Shield work continues – the US Commerce Deputy Assistant Secretary, Ted Dean, has been talking to EU Data Protection Commissioners on how to make the Shield work the best possible way. Part of its success depends on a favourable view by the DPAs, part on the understanding and awareness of consumers (p.18) and part on the take-up and compliance by US business (p.1). On p.15, take a detailed look at how Privacy Shield obligations affect vendor management.

An additional important point, specifically for banks and telcos that cannot take advantage of the Shield, is the future of EU model contractual clauses. The case on their legality will now be heard in February next year (p.28). The EU may consider expanding the scope of the Privacy Shield, but for now, companies that do not want to apply for the Shield for one reason or another are in a limbo.

The right to data portability under the GDPR is still not well understood. Read on p.12 a financial services perspective on this new concept.

Organisations now have until September next year to organise compliance with the data protection law in the Philippines. Implementing regulations have been issued, and those processing data of at least 1,000 individuals must notify (p.19).

Genetic privacy poses many questions that are not governed by existing laws. Also the GDPR's approach in this field is somewhat unclear. While there are some guidelines on genetic data, genetic enhancement and personalized medicine, sufficient rules are lacking (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Privacy Shield... from p.1

the first two weeks following the launch, the Department of Commerce posted less than 40 company listings. Meantime, this number has increased to 200[2]. Another 300 companies are "being reviewed", and around 400 companies have submitted "some information." Department of Commerce officials are still optimistic that they will surpass the EU-US Safe Harbor with its 4,000 US companies listed as data importers.

Glass half empty or half full?

It is probably too early to tell, but a new International Association of Privacy Professionals survey[3] underscores the climate of uncertainty around the newly approved EU-US Privacy Shield. It finds that only 34% of privacy professionals whose companies transfer data from Europe to the US said they expected their businesses to adopt the PS framework data flow. There are various reasons for their reluctance to self-certify. Some US data importers are concerned that the European Court of Justice (ECJ) will invalidate the PS framework, as it did last year with Safe Harbor. Others don't want to jump ahead of their competitors. Another group of data importers are concerned about the level of scrutiny by the Federal Trade Commission (FTC) once they make it on the list, or are wary of proceedings launched against them in Europe through Data Protection Authorities (DPAs). Many Europeans had rebuked the EU-US negotiating team for failing to include sufficient safeguards for the privacy of EU personal data in the hands of US organizations (in particular, the ease with which US law enforcement and other agencies could access them). To some extent, that has undermined the credibility of the PS framework even before its launch.

The DPAs don't make the decision easier. The German State DPA of North Rhine Westfalia issued its own "guidelines" for data exporters,[4] dated 12 September 2016, warning companies that all data exporters in its jurisdiction must verify :

- that the data importer under the PS is registered on the list and that the certifications are valid;
- The data importer has fulfilled its "notice" and "onward transfer obligations"; and
- that the German laws for general controller-processor data processing are implemented (Sec. 11 German Data Protection Act).

The data exporter needs to document that it has complied with all these obligations before sending any data to the data importer. Currently, there is no need to notify the relevant DPA, but the DPA of North Rhine Westfalia has put companies on notice that they will raise any issues with the PS either directly with the data exporters in their jurisdictions and/or in the framework of the annual review of the PS with the US government.

From a practical standpoint, PS applicants who thought that they could simply resubmit their existing filings and policies under the old Safe Harbor realize that they face much more compliance work and it is more expensive than originally thought. The PS triggers various annual fees and certification renewals, and the internal compliance costs can be expensive. On top of it, there is lack of certainty as to who can file, what is required for a filing and what consequences result from self-certifying.

> As was the case with Safe Harbor, not every data importer is eligible to self-certify

Who is eligible for the Privacy Shield?

As was the case with Safe Harbor, not every data importer is eligible to self-certify under the PS. The PS Principles state that the organization must be subject to the jurisdiction of the FTC or the Department of Transportation. The Department of Commerce provides the following clarification on its PS website: "The FTC does not have jurisdiction over most depository institutions (banks, federal credit unions, and savings and loan institutions), telecommunications and interstate transportation common carrier activities, air carriers, labour associations, most non-profit organizations, and most packer and stockyard activities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances. Note that to be transferred in reliance on the Privacy Shield, personal data must be processed in connection with an activity that is subject to the jurisdiction of at least one appropriate statutory body listed in the Framework."

This definition triggers different questions: For instance, which non-profits can self-certify under the PS? The FTC Act covers all business' unfair trade practices but generally does not cover actions of non-profit organizations. However, a US Supreme Court decision found that where there is substantial economic benefit to its members, a site may be deemed commercial and governed by the FTC Act. Another area of concern is whether over-the-top, voice over Internet (VOIP) service providers are entitled to file to the extent they fall under the jurisdiction of the Federal Communications Commission (FCC) or the joint jurisdiction of the FTC and the FCC. The Department of Commerce doesn't decide these legal issues, but refers them to the FTC's PS team to determine whether a company is eligible for the PS. The self-certifying organization could thus face significant delays before they are admitted to the PS list. Not knowing whether they will make it on the list leaves such would-filers in an untenable limbo situation. Moreover, a recent decision by the US Court of Appeals for the Ninth Circuit, which could be interpreted as drastically reducing the FTC's jurisdiction over certain telecommunications companies, further complicates determining PS eligibility.

Privacy Shield Statements differ significantly

The Department of Commerce requires URLs for the Privacy Policy at the time of the self-certification. PS

statements for HR data must only be uploaded and are not published on the PS list. It is not surprising that many small companies do not post lengthy PS statements that a data subject would expect from large US corporations. However, the current standards set by self-certifying entities vary. Some data importers post general Privacy Policies with short paragraphs on the PS, stating that they will abide by the Notice and Choice and the other PS Principles. Other PS statements or Privacy Policies are much more detailed. The Notice Principle in the PS Principles lists 13 different categories of information that must be notified, such as "the type or identity of third parties to which it discloses personal information, and the purposes for which it does so." As far as one can conclude from the posted policies, none of the filers provides a large level of detail, e.g., by disclosing the full names of the parties that receive personal data under the PS. Not all of the links posted on the PS list work, and the distinctions between HR and Non-HR data in many policies are far from clear. Some companies treat EU data subjects and US residents on equal footing in their policies, some don't.

Struggling with onward transfers and the deadline

The PS's Onward Transfer Principle (Principle 5) triggers a lot of due diligence for the US companies. This Principle states that a data importer must enter into a contract with the third-party (e.g., a service provider or "agent") that has access to the data from Europe. The PS Principles avoid the EU terminology "data processor" and use the term "agent" instead. Including an "agent" into the chain of data flows will require significant due diligence before any data transfer under the PS since the data importer can be held responsible for the actions of the agents that violate the PS. A "Due Diligence Sheet for Agents" or similar compliance measures are advisable for the data importer as a first step to demonstrate due diligence. In addition, the contract with the agent must stipulate that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual to the data controller. It must also contain a clause that the third party will provide the same level of protection as the PS Principles. The third party must further notify the data importer if it can no longer meet this obligation. Specific contractual stipulations must address what occurs if the third party ceases processing of the data. There is no template for such an agreement. The data importers are left largely on their own. The regulators can demand copies of these agreements.

This brings us to the issue of the grace period that has caused some confusion. The PS Principles require that these contractual requirements for onward transfers must all be in place when the self-certification is submitted. The Department of Commerce grants a grace period of nine months for the data importer to bring their contracts with its vendors and other third parties in line with the PS Onward Transfer requirements. After some initial confusion about the deadline for this grace period, the Department of Commerce has clarified by way of FAQ that only data importers that submit their self-certification by September 30 can take advantage of this grace period. Unfortunately, various data importers were not yet ready for this major step. It is not clear whether the department will grant temporary exemptions from the onward transfer principle after September 30 so that these data importers will be able to enter into the necessary contractual requirements with the relevant third parties. Additionally, companies that make the September 30 deadline but are unable, for whatever reason, to enter into the necessary agreements with third parties within the nine month grace period will be in the unenviable position of being both out of compliance with PS and required to destroy any PS-subject data collected during such nine-month period of time.

An ongoing process

Compared to the Safe Harbor principles, the PS follows a much more structured approach. It provides for various mechanisms individuals can use to lodge complaints against a data importer in the US. If the company does not resolve the issues identified, then there is an arbitral panel proceeding that these individuals can use. All data importers must have an internal compliance system in place when they self-certify with the Department of Commerce. This dispute mechanism must function properly and all fees for any third-party dispute resolution must be paid by the company. Individuals, for instance, who want to know what the data importer has stored about them, must be able to launch inquiries from day one. The PS policies and statements posted vary widely, although there is not much room for trial and error. If a company joins the PS and later decides to leave it, the company still must adhere to the PS Principles with respect to the personal data the company has collected while it was PS-self-certified. Moreover, if a company is deleted from the PS list, it has to purge or return all the EU personal data it obtained through the PS. That could create a major compliance burden down the road, especially when third parties had access to the personal data.

AUTHOR

Axel Spies is an attorney at Morgan Lewis LLP in Washington DC and is an international data protection expert and blogger (www.blog.beck.de)
Email: axel.spies@morganlewis.com

REFERENCES

1 www.privacyshield.gov/welcome
2 www.privacyshield.gov/list
3 Cited by www.scmagazine.com/survey-34-of-privacy-pros-expect-their-companies-to-certify-under-privacy-shield/article/519777/ (9 August 2016)
4 In German: ww.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt/Eingangsseite/EU_US_Privacy_Shield_Text_komplett.pdf

13 QUESTIONS AND ANSWERS ON EU-US PRIVACY SHIELD IMPLEMENTATION

1. What are the main points in the Department of Commerce's review process for EU-US Privacy Shield applications?

- The review team expects plain language, clarity, and consistency.
- Applicants should provide the data requested for each type of data they hold, for example human resources and marketing data.
- An applicant's certification application should cover all 13 elements requested by the Department of Commerce. If not, the review team will contact the applicant to discuss the missing elements.
- If not transferring personal data abroad, say so.
- Availability/visibility of Privacy Shield policy. Make clear where the policy is available for staff and public to see.
- Ensure that you register with a dispute resolution provider or the DPA Panel at the International Trade Administration.

2. What is the scope of self-certification regarding dispute resolution: Can a company self-certify for its dispute resolution provider for only a specific product and/or functions?

A dispute resolution provider must cover everything.

3. Can more data types be added to a Privacy Shield certification at a later stage?

Yes you can update your certification at any time. Whatever personal data you are covering, you need a privacy policy.

4. I am not sure if my insurance company falls under Federal Trade Commission jurisdiction (because insurance is regulated by the 50 states, not the FTC).

If you are not sure about FTC jurisdiction, contact the Privacy Shield administration at trade.gov with as much detail as possible and the FTC will respond from the General Counsel's office. This process should take about a week.

5. Do you recommend a specific type of browser to submit a company's certification?

Use Google Chrome to submit your certification.

6. Do 3rd party sub-processors need to be certified under the EU-US Privacy Shield?

No they do not need to be certified. But you do need a contract with them that provides the same level of protection as the Privacy Shield.

7. Can we demonstrate accountability by using EU standard model clauses with sub-processors?

Yes, to satisfy contractual requirements as they are sufficient.

8. Can Human Resources and marketing data be in one Department of Commerce certification?

Yes, they can be in one Department of Commerce certification. Upload your URL and describe your policy in a short version.

9. What are the common mistakes in the certification process?

- Not giving the URL
- Not registering with a dispute resolution body
- Not including all the points on the list.
- Not mentioning onward transfers
- Retaining references to the Safe Harbour.

10. How do I know if my certification is confirmed?

The Department of Commerce will confirm this by email.

11. May I use my own design for a Privacy Shield logo?

No. The Department of Commerce is working on a logo.

12. What if our privacy policy is on our company's customer portal?

You still need to send your privacy policy to the Department of Commerce. If you have a customer-facing website, also include the privacy policy there. Make clear it applies to EU sourced data. You can also put the privacy policy on your customer portal if that is the way individuals access it.

13. Do different rules apply to data controllers and data processors?

No. The privacy framework does not distinguish between controllers and processors, so the same rules apply. You must inform customers about their access rights and refer requesters to the appropriate place where they may find relevant information.

• *The questions and answers, reported by Stewart Dresner, are based on a DLA Piper webinar on 22 September 2016 with Caitlin Fennessy, US Department of Commerce, Jennifer Kashatus, DLA Piper and Kate Lucente, DLA Piper.*

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK