Pepper Hamilton LLP
Attorneys at Law

TRAVERS SMITH

# Data Protection Update: Joint Webinar with Travers Smith Q&A

April 2016

**Sharon R. Klein** | kleins@pepperlaw.com

**Alex C. Nisenbaum** | nisenbauma@pepperlaw.com

**Dan Reavill** | dan.reavill@traverssmith.com

On March 9, 2016, leading UK and U.S. law firms, Travers Smith and Pepper Hamilton held a joint webinar to discuss the new "EU-U.S. Privacy Shield", highlight possible new compliance burdens and examine the alternative mechanisms being used to allow export of personal data from the UK / Europe to the United States, and learn about the issues which both UK and U.S. businesses will have to plan for in order to comply with the upcoming GDPR.

The webinar recording and PowerPoint slides are available here.

There were a number of questions that were submitted by the audience but could not be addressed due to time constraints. Below are the answers from the speakers to those questions.

**Q: The ECJ decision has invalidated transfer of data based on Safe Harbor, so data can no longer be transferred to US based on SH. Does this also affect transfer of personal data to US, based on pre-existing data processing agreements with US partners?**

A: This would affect transfer of personal data to the US if the gateway on which a data processing agreement was reliant for compliance with European data protection legislation, was the fact that the US data processor was signed up to the Safe Harbor. However if the data processing agreement is based on another "transfer gateway" such as the use of model clauses, then it should not be affected by the invalidation of the Safe Harbor agreement.

**Q: If implemented, will the GDPR in any way affect the way data processing agreements are now entered into between Data Processors and Data Controllers, in particular, having regard to the fact that Data Processors will also be directly subject to the GDPR alongside the Data Controller?**

A: We don't think that the GDPR will affect the way data processing agreements are entered into between data processors and data controllers. As with current European data protection law, data controllers will still need to put in place binding contracts with processors. However three things to note:

i) under the GDPR the controller will have to ensure that it only uses processors which provide sufficient guarantees that they will implement appropriate technical and organisational measures which meet the requirements of the Regulation and protect data subjects' rights – so it will have to make sure that it effectively polices its relationships with processors, and maintains oversights of their processes and procedures;

ii) the GDPR is very prescriptive about what needs to be included in contracts with data processors, including the data processed, the duration of processing, and obligations on processors to assist with audits and security breach responses;

iii) data processors may want to change the way liability is dealt with in data processing agreements, given that they will be directly liable under the GDPR for fines and claims by data subjects which result from non-compliant processors of personal data (which is not the case currently).

**Q: Can you comment on the Electronic Frontier Foundation announcement of inadequacies in the PS?**

A: Like a number of other consumer privacy advocates, the Electronic Frontier Foundation (EFF) has questioned whether the Privacy Shield contains sufficient mechanisms to protect European citizen personal data from mass surveillance by U.S. intelligence agencies. For example, almost immediately Max Schrems stated that the protections of the Privacy Shield were inadequate. See http://www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277. Of course, as one of the major drivers of the invalidation of Safe Harbor, whether the EU authorities will determine that the Privacy Shield contains adequate protections sufficient to overcome the issues identified by the Court of Justice of the European Union (CJEU) has always been a big question. The U.S. has maintained that after the Snowden revelations, the U.S. placed new limits on bulk collection of data for surveillance purposes via presidential order that the CJEU failed to consider. We will see when the Article 29 Working Party delivers its opinion whether it sides with privacy advocates like the EFF or finds that the U.S. has demonstrated it has provided appropriate assurances of protection from U.S. law enforcement and intelligence agency activity.

**Q: What is the status of the proposed Binding Safe Processor Rules (BSPR) that the Working Party is considering?**

A: The BSPR were set up in 2012 as a tool to help frame international transfers of personal data that are originally processed by a processor on behalf of an EU controller and under its instructions, and that are sub-processed within the Processor's organisation. They were adopted by the Article 29 Working Party (which is the European body which represents EU data protection authorities) on 19 April 2013. Under an arrangement similar to binding corporate rules for group wide data transfers, the BSPR allow companies to transfer personal data overseas that they process on behalf of other organisations. The rules are still in place and still work, in the same way that binding corporate rules are also still a valid transfer mechanism in the appropriate circumstances. However there is a

possibility that data protection authorities will want to re-visit them in light of the GDPR, once that is in force, though to date nothing has been said about that.

### Q: Didn't HR 2048 which is not an Executive Order, end the bulk collection of data?

A: HR 2048, the USA Freedom Act, did impose new limits on bulk collection of telecommunications metadata on U.S. citizens. Privacy advocates in both Europe and the U.S. have pointed to other mechanisms that authorize surveillance of persons outside the U.S., such as Executive Order 12333 and the FISA Amendments Act of 2008, as problematic and out of step with protections that would be required under the decision by the Court of Justice of the European Union that invalidated the Safe Harbor.

### Q: How far do we go with EU personal information? The standard metadata is understood, do we need to go further with including age, sex, town?

A: In contrast to U.S. laws, which generally define personal information more narrowly with respect to specific types of data, the General Data Protection Directive and future General Data Protection Regulation define personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." This is incredibly broad. Accordingly, controllers/processors should treat all information relating to an individual as personal data unless it has been anonymized in accordance with regulatory guidance, for example from the UK Information Commissioner's Office. See https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation .

### Q: For organisations like ours which require consents for marketing, what should we be looking doing to ensure we meet the new consent requirements?

A: Under the GDPR, consent will have to be freely given, specific, informed and an unambiguous indication of the data subject's wishes, either by a statement or a clear affirmative action which signifies their agreement to the processing of their personal data. In practice this seems to mean that consents must be given by way of a positive act and it will no longer be possible to rely on "soft opt-ins", silence, inactivity or pre-ticked boxes.

In addition, further requirements for valid consent are that:

- The consent must be distinguishable, clear and not bundled with other written agreements or declarations
- Data subjects are informed that they have the right to withdraw their consent at any time, with simple methods available for withdrawing consent
- Separate consents are obtained for distinct processing operations.

If the data that you have collected and processed to date has not been collected on the above basis (e.g. consent has been obtained using soft opt-ins) then, in advance of the GDPR coming into force, you will have to contact your existing customers afresh in order to renew consents. You should also check your data collection processes and notices on websites, together with privacy policies, to check that they comply with the new requirements.

### Q: What if the data processor is not aware of the content of the controller's data? In the example of an eDiscovery firm who collects and processes data pursuant to a discovery order.

A: Neither the privacy shield nor the General Data Protection Directive require a processor to have knowledge for the applicable legal requirements to apply. Moreover, the new General Data Protection Regulation that should take effect sometime in 2018 will provide that processors are directly liable for violations of the Regulation, without providing an ability to hide behind the data controllers. As a practical matter, if a company is transferring data from the EEA to the US that could contain personal data, an appropriate, valid mechanism for transfer such as model clauses should be used.

### Q: Can you elaborate on the definition of personal data - it seems very different from how some U.S. states denied PI?

A: In contrast to U.S. laws, which generally define personal information more narrowly with respect to specific types of data, the General Data Protection Directive and future General Data Protection Regulation define personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." This is incredibly broad. Accordingly, contollers/processors should treat all information relating to an individual as personal data unless it has been anonymized in accordance with regulatory guidance, for example from the UK Information Commissioner's Office. See https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/.

### Q: Is there any risk of participating in the Privacy Shield while having Model Clauses?

A: No, there is nothing that would prevent a company from using both model clauses and the privacy shield to comply with personal data transfer requirements.

### Q: Are there vendors for privacy shields?

A: Companies will self-certify compliance with the Privacy Shield Principles. While there may be third parties such as legal counsel that can assist with such organizational certification, there are no third party vendors that can independently confer indicia of compliance with the Privacy Shield.

### Q: Where personal data is housed on a database in the EU but is made available in for example read only access in the United States, would this constitute a transfer to U.S.?

A: In the eyes of data protection laws in this context, data accessible overseas on a read only basis is treated in exactly the same way as downloadable material. Consequently, the answer to your question is "yes" (although technically speaking is accessing the data in the States which triggers the problem, rather than merely making it available for access in the EU).

In contrast, if personal data was to be loaded from the EU onto a publicly accessible website hosted in the EU which was only intended for EU based citizens to access, but which could be discovered and read by a person based in the US if they made the effort to search for the site, then the mere loading of the data onto the website would not in itself constitute a transfer. As usual much depends on the particular context of the situation: what the intention was of the party uploading the data in terms of who should access it; how that data can be accessed, and how easily it can be found.

Another point to watch out for is when data is in transit or routed through a third country on its way to another EEA country – this wouldn't constitute a transfer either.

### Q: In terms of data breaches being reported and having to contact all subjects involved does it specify how subjects must be notified and what must be included in the notification?

A: If a data breach notification is required to be sent to data subjects under the new General Data Protection Regulation (recall that such notice is only required in the event it is determined that the breach "is likely to result in a high risk [to] the rights and freedoms of individuals"), the notice must be in clear and plain language and contain at least the following information:

- The name and contact data of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including where appropriate, to mitigate its possible adverse effects.

The Genera Data Protection Regulation does not specify how subjects must be notified, but does provide that the notice is not required to be provided if the notice would involve disproportionate effort. In such situations, the Regulation requires a public communication or similar measure where data subjects are informed in an "equally effective manner." In the U.S., we would consider such measures to include dissemination in widely circulated media and an announcement on the controller's website regarding the breach.

**Q: Where an online transaction is being paid for by an EU citizen through a credit card that goes to a merchant's processor outside the EU, does that processor need to be observant of the requirements or is the data transfer part of the actual transaction?**

A: Please correct me if I'm wrong, but I think you are asking whether merchant processors located outside the EU will have to comply with the GDPR once it comes into force.

Under both current law and the GDPR, the merchant processor is probably acting as a "data processor" on behalf of its customer (i.e. the operator of the website). Article 3 of the GDPR says that a data processor based outside the EU will be required to comply with the GDPR if it is processing the personal data of data subjects who are inside the EU, provided that the processing relates to the offering of goods and services to data subjects in the EU.

Since the merchant processor's activities relate to goods or services offered (by the website operator) to an EU citizen (who we assume is based in the EU for the purpose of your question), then yes, the processor would come within the GDPR's territorial scope.