Cooley

October 15, 2015

Last week, Europe's highest court, the Court of Justice of the European Union, (CJEU) declared the Safe Harbor framework invalid. You can read more about the decision in our previous alert here. Although it is unlikely that national data protection authorities will move to immediate enforcement—and it is believed that companies will be given time to get their house in order—the law has changed with immediate effect and organisations relying on Safe Harbor need to act quickly and practically. In essence, there are two options: (i) keep personal data in the EEA; or (ii) find alternative methods of safely transferring data to the US.

What does this mean for online retailers?

With online retailers collecting and using large quantities of personal data not only to conclude online transactions but also to advertise and promote, often transferring this data to the US, the loss of the Safe Harbor Scheme means alternative ways of staying compliant with the EU Data Protection Directive need to be employed. Pseudonimizing or anonymizing data may not be appropriate for the online retail industry, but other alternatives do exist. There is ample data at stake: an extensive review of business processes, systems, controls, and agreements (including customer, supplier and personnel agreements) is advisable.

Things to consider now

Review current data flows

As a first step, companies should review what data are being processed and where. Is personal data leaving the EEA and if so, in what format? Only data from which individuals can be identified or are identifiable are subject to the restrictions on data transfers outside the EEA. Online retail companies based in the US will most likely be receiving personal data from the EEA-based limbs of the online retailer - when customers input their data -US companies are likely capturing this from EEA sites. Some of this data will usually be personally identifiable, such as the data related to online log-ins. Other data may be anonymised or key-coded, such as the data related to any financial transaction. A retailer may also be providing personal data to advertising companies who will be using the data to track customer user habits and/or to personalise online advertising campaigns.

Consider alternative transfer mechanisms

It is important to remember that Safe Harbor is not the only method of legitimising data transfers to the US – it was simply one that was regularly used by businesses wishing to transfer data outside of the EEA in compliance with EU rules.

a. Consent

One of the mechanisms which effectively exempt data from the restrictions on transfers outside the EEA is consent. To be valid, the consent must be fully informed, specific and freely given.

What this means in practice in the online retail world is that consumers must be provided with details of where data are to be transferred, including the fact that the regimes protecting data in these other countries may be less rigorous than that in the EEA. Individuals must also be able to withdraw their consent to the transfer of their data at any time. Finally, consent must be clearly signified: it cannot be inferred from a failure to respond. This consent could be sought at the confirmation of purchase page, or where the customer is asked to set up an online account with the retailer.

b. Model Contractual Clauses

Another way of legitimising data transfers to the US is for the data exporter (the entity in the EEA transferring the data outside the EEA) and the data importer (the entity outside the EEA receiving the data) to enter into an agreement incorporating the Model Contractual Clauses (contractual provisions applying EEA data protection

obligations on the contracting parties). At present there are only controller-to-controller and controller-to-processor clauses available, which means that the data exporter (the entity in the EEA transferring the data) must be a data controller, i.e. a person who, either alone or jointly, determines the purposes for which and the manner in which data are, or are to be, processed. In most cases, the company and the site will be joint data controllers, and so can enter into the controller-to-controller form of Model Contractual Clauses.

In some EEA Member States (e.g., Belgium and Spain) executed Model Contractual Clauses need to be lodged with or notified to the State's data protection authority (DPA) prior to the transfer of any data, and in a few Member States (e.g., Austria, France, Ireland, Romania and Slovenia) the Clauses need to be approved by the DPA prior to use. The time taken to approve Clauses can vary significantly, so extra time should be allowed to complete these formalities prior to transfer.

c. Binding Corporate Rules

For US companies with EEA subsidiaries, Binding Corporate Rules (BCRs) offer an alternative transfer mechanism for data transfers to the US. BCRs are legally enforceable rules that ensure that a high level of protection is applied when personal data are transferred between group companies, whether within or outside the EEA. Companies can construct these themselves and they are often based on pre-existing data transfer agreements. However, BCRs need to be approved by local DPAs and the approval process can be lengthy so again, time should be allowed to complete the approval process prior to transfer.

Final thoughts

Following the CJEU's ruling, many of the DPAs have stressed the need for a coordinated response by Member States. Guidance is anticipated and it is likely that companies will be given a grace period to legitimise their data transfers. However, companies should start considering their options now; as mentioned above, some of the alternatives have a potentially long lead-in time. How companies decide to move forward will depend on many factors, including the nature and size of operations - there is no "one size fits all" solution. Companies needing tailored advice on possible solutions to suit their business needs should contact Sarah Pearce.

Please contact Cooley's London Privacy & Data Protection team, which is led by partners Ann Bevitt, Mark Deem and Sarah Pearce to clarify options in light of the ruling and practical alternatives to suit your business needs. They offer multi-disciplinary depth and breadth of experience to clients in data protection, privacy by design, data breach management, incident response, breach preparedness, and related litigation, especially in large breaches and those with multi-national issues.