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—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 the social media industry?

It is likely that the big players in social media have been working on their 'Plan B' for some time and will have user agreements in place to implement the safe transfer of data to the US, or will have EU-based servers as backups. However, they might not have it all figured out just yet – after all, the ruling was not expected for another couple of months. Although model contracts will do the job for now, national data protection authorities (DPAs) are likely to examine these in greater detail, and may, in some cases, see them as an inadequate "band-aid solution" to a large flesh wound. It is important to remember that it is not just the Safe Harbor framework that was scrutinised, but the way in which the US treats data it receives from the EU; all routes, including other previously trusted alternatives, will be the subject of a closer inspection as to data protection "adequacy".

For companies operating in the big wide world of social media, a plethora of valuable data is at stake: data created via social media posts; web searches; and behavior patterns monitored by cookies, to name a few.

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 identifiable are subject to the restrictions on data transfers outside the EEA. Some data may be personally identifiable such as user photos, while other data may be more easily anonymized or key-coded, such as user contact details.

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, however, 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 exempts data from the restrictions on transfers outside the EEA is consent: to be valid, consent must be fully informed, specific and freely given.

What this means in practice is that individuals 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.

Generally speaking, social media users should be presented with clear notices, pop-ups or tick boxes at the point at which they are requested to submit data, setting out the data controller's intentions with respect to that data. Explicit consent in an online environment must also be recordable, so that it is accessible for future reference. Privacy policies should be updated to reflect this.

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 many cases, a social media company and the website 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 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 noted 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.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.