Cooley

October 13, 2015

Last week Europe's highest court, the Court of Justice of the European Union (CJEU) declared the Safe Harbor framework invalid. Many life sciences and biotech companies relied on Safe Harbor to legitimise transfers of personal data from the European Economic Area (EEA, i.e. the EEA Member States plus Iceland, Liechtenstein and Norway) to the US. What should these companies be doing now in light of the CJEU's decision?

Review current data flows

As a first step companies should review what data are being processed and where. Are data leaving the EEA personally identifiable or anonymised or key-coded (and if the latter, who has the key)? Only data from which individuals can be identified are subject to the restrictions on data transfers outside the EEA.

Life sciences and biotech companies based in the US may be receiving data from a number of organisations based in the EEA, such as clinical research organisations (CROs), the sites conducting the research and investigators. Some of this data may be personally identifiable, such as the data provided by the CRO to allow the company to select the site and/or investigators to conduct the clinical research. Other data may be key-coded, such as the data of the patients undergoing the clinical trials.

Consider alternative transfer mechanisms

Consent

Safe Harbor is not the only method of legitimising data transfers to the US. One of the derogations which exempt 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.

All patients undergoing clinical trials are provided with detailed information about the research and required to give their consent to their participation. These consents should be reviewed, and if necessary revised, to ensure they allow for the transfer of data to the US.

Whether patient data are personal data (and therefore subject to the restrictions on transfer) will depend on a number of factors, including the phase of the research project. For example, in Phase 1 projects, patient data are likely to be anonymised. However, even at this stage if the drug being tested has an orphan drug designation (i.e., the disease being investigated affects less than 5 in 10,000 people), anonymised data which shows, for example, gender, age, disease stage and location may be personally identifiable.

Patient data are not the only data that may be transferred from the EEA to the US. For example, the CRO may (as noted above) provide the company with data on sites and investigators which is likely to contain personal data, such as the data of the individual medical professionals who will be involved in the research. The fact that this information may be publicly available does not mean that it can be freely transferred to the US; it is still subject to the restrictions on transfer. As the company has no direct contact at this stage with these individuals it cannot obtain their consent. Instead, it should ensure that there is in its contracts with CROs confirmation by the CROs that they have the necessary consents from these individuals, or legitimise the transfer of those data in some other way (see below).

Accordingly, companies should review their existing contracts with CROs to see if they contain such confirmations and should ensure that any new contracts entered into with CROs do so. If existing contracts do not have the necessary confirmations companies should consider alternative transfer mechanisms (see below).

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 the site can enter into the controller-to-controller Model Contractual Clauses. However, CROs are generally considered to be data processors and so there are no Model Contractual Clauses currently available for them to enter into.

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.

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. 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, 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 their operations—there is no "one size fits all" solution. Companies needing tailored advice on possible solutions to suit their business needs should contact Ann Bevitt for further assistance.

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.

Key Contacts

Ann Bevitt London	abevitt@cooley.com +44 (0) 20 7556 4264