Changing Rules on Data Transfer from the EU

The introduction of the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") was a painful process for many companies as databases were stripped, new practices introduced and consents to hold data obtained. Some requests were ignored or forgotten and valuable contact details had to be deleted. For clinical trial practice, however, it was a welcome reform. The previous law was a directive that had to be introduced separately in each member country with the inevitable local variations, which led to additional costs and frustrations. A regulation has automatic effect across the EU and should be interpreted in the same way in each Member State.

The GDPR prohibits export of personal data to countries that do not provide individuals with enforceable privacy rights over their data, but transfers to countries with levels of protection for personal data that the Commission deemed adequate are permitted and minimal additional processes are required. Until recently, the US was on the approved list. While some privacy lawyers had some doubts as to whether the US Privacy Shield really did offer sufficient protection, industry was generally pleased and of course in the context of the international pharmaceutical industry and cross-border clinical trials, it was a huge relief. This summer, however, the European Court invalidated the adequacy finding by the European Commission for the US, throwing the whole situation into uncertainty (Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems).

The case known as Schrems II is highly complex, but fortunately the judgement is quite clear. The lawyer who brought the case, Max Schrems, had previously brought a case that struck down the previous data transfer system between the US and EU, known as the Safe Harbour scheme. This second case focussed on two points; firstly the Privacy Shield which had been introduced in response to the demise of the Safe Harbour scheme and was meant to address its shortcomings. He argued successfully that this new scheme gave primacy to US rules permitting electronic surveillance over the rights of individuals required by the EU rules, and that this meant that the protections offered were not in fact adequate. Secondly, he argued against the alternative form of protection for exported data, the Standard Contractual Clauses. These are a set of contractual terms laid down by the Commission which, if included in a contract, are intended to ensure that the parties handle personal data in a manner that provides adequate protection to the EU citizen whose data has been exported, and in fact predate the GDPR (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en). As an example, in his suit he challenged the use of such clauses by Facebook. In this part of his case, he was not successful. The court found that the clauses were a valid way in which to protect citizens' rights and that their use could continue; however, there was a sting in the tail. The court ruled that in using the Standard Contractual Clauses, a party had to also consider the context of that use and the legal protections offered by the country to which export was to be made. In particular, consideration had to be given to the extent to which public authorities in the destination country had the right to access the exported personal data. If the data controller in the EU was dissatisfied with the level of protection offered, then the transfer should not take place even where the foreign party had accepted the Standard Contractual Clauses. As the European Court has specifically said that the US laws do not provide adequate protection, then this would seem to automatically prohibit the use of the Standard Contractual Clauses in relation to export of data to the US.

Where then does that leave us? The court judgement, unlike a new piece of legislation, does not have a transition period. It takes immediate effect, so companies must consider their current contracts and practices and not just future activities that are being planned. Clearly any reliance on the Privacy Shield must stop immediately. Companies must undertake due diligence to consider whether the countries to which they are transferring data do offer appropriate data privacy, even where the Standard Contractual Clauses are used, and ideally not transfer data to such countries. Both the US and the EU have said that they are working on an alternative to the Privacy Shield and the EU has said that it is working on revising and strengthening the Standard Contractual Clauses. Companies should keep an eye out for these changes, but in the meantime should review their consent forms and contracts to ensure that the data subjects are aware of the situation, and give full consent in these changed circumstances. Wherever possible, personal data should be held and processed within the EU and not transferred out of the block. Additional clauses in contracts could be considered, such as greater use of anonymity, encryption and prohibitions on transfers to other companies, but these will need to be considered on a case by case basis.

A further issue on the horizon for international trials is the potential impact of Brexit. The UK is currently compliant with all the EU rules on data protection and will incorporate such laws automatically into UK law at the end of the year. The UK government has previously indicated that the GDPR regime would continue post-Brexit. This should mean that there should not be any immediate impact on the acceptability of the UK as a data transfer destination; however, as a non-EU country, contracts will need to be revised to include the Standard Contractual Clauses and companies may have to appoint a data representative within the EU. Moving forward, the UK will no longer be subject to the European Court and so it is to be

expected that there will be different interpretations over time by UK courts. While new UK laws could again be anticipated over time, it seems that this may be coming sooner than originally thought. The UK government published its National Data Strategy on 9th September (https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) and this has raised a number of concerns in Brussels, in particular in relation to government access to and use of personal data which may well conflict with the Schrems judgement. It is, of course, early days and the strategy document is only a first step on which comment is now being sought, but it is certainly a complicating factor.

So while many may have thought once they had addressed the GDPR reforms and updated their processes to accommodate those, that they could forget about data protection for a while, it seems that is not to be the case and that we are again looking at substantial upheaval ahead.

Patricia Barclay

Patricia Barclay studied law at the Universities of Edinburgh and Oxford before embarking on a career in the life science industry. She held a number of senior positions at Pfizer before becoming General Counsel of Vernalis plc. She subsequently served as General Counsel of the Ferring Group and of Solvay Pharmaceuticals before setting up Bonaccord a law firm dedicated to supporting the scientific community. Bonaccord has won many awards including as UK Life Science Law Firm of the Year. In addition to her legal work Patricia is an active business mentor and teaches at both academic and professional levels.

Email: patricia@bonaccord.law