Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Issues Facing Life Sciences Cos. After EU-US Safe Harbor

*Law360, New York (October 20, 2015, 11:38 AM ET) --*

Pulina Whitaker

Paul Ranson

Life sciences companies who routinely transfer personal data, typically sensitive personal health data, from within the EU to the U.S. commonly rely — in addition to consent, model clauses and public health benefit exemptions — on safe harbor to validate such transfers. A recent case may require that strategy to be reconsidered.

In Maximillian Schrems v. Data Protection Commissioner (case C-362/14), the European Court of Justice ruled that the European Commission decision approving the safe harbor program is invalid. It also ruled that EU data protection authorities do have powers to investigate complaints about the transfer of personal data outside Europe (whether by safe harbor-certified organizations or otherwise but excluding to countries deemed as having "*adequate*" data protection laws according the EU) and where justified, can suspend data transfers outside Europe until their investigations are completed. As we described in our previous article, the European Commissioners plan to issue guidance to safe harbor certified companies within the next couple of weeks.

In the meantime, life sciences companies who routinely transfer personal data, typically sensitive personal data, relying on safe harbor should be considering alternatives to safe harbor.

**Safe Harbor is "*Invalid*"**

The ECJ declared that the European Commission's decision to approve the safe harbor program in 2000 is "*invalid*" on the basis that U.S. laws fail to protect personal data transferred to US state authorities pursuant to derogations of "*national security, public law or law enforcement requirements.*" Further, EU citizens do not have adequate rights of redress where their personal data protection rights are breached by U.S. authorities.

In the last two years, the European Commission and various data protection working parties have discussed ways to improve the safe harbor program and strengthen rights for EU citizens where their personal data is transferred to the U.S. Recently, the U.S. and EU finalized a data protection umbrella agreement to provide minimum privacy protections for personal data transferred between EU and U.S. authorities for law enforcement purposes. The umbrella agreement will provide certain protections to ensure that personal data is protected when exchanged between police and criminal justice authorities of the U.S. and EU. The umbrella agreement, however, does not apply to personal data shared with national security agencies.

The powers of national data protection authorities are significantly strengthened by this decision. They could suspend some or all personal data flows into the U.S. in serious circumstances and where they have justifiable reasons for do so. There is a risk that a data protection authority could order that that data transfers by an international organization outside Europe be suspended from that jurisdiction whereas data transfers in other European jurisdictions are permitted. To mitigate this risk, the European Commission is entitled to issue EU-wide “adequacy decisions” for consistency purposes.

**Other Options to Transfer Personal Data to the U.S. After Safe Harbor**

Safe harbor-certified organizations should note that there are other options to transfer personal data to the U.S., including ensuring that express consent is obtained for both primary and secondary uses and the use of Binding Corporate Rules or EU-approved model clause agreements. Organizations who partner with safe harbor-certified organizations may wish to discuss these other options with their partners. There is, however, a risk that this decision could affect Binding Corporate Rules or EU-approved model clause agreements (for the same ECJ concerns regarding national security). Relying on consent alone, however, can be problematic if the validity of consent is challenged as not being freely given (e.g., if it is a condition of a service or a benefit), it is not fully informed or if consent is qualified or withdrawn.

**Some Key Issues for the Life Sciences Sector**

Many pharmaceutical and medical device companies are, themselves, safe harbor-certified and/or they partner with or are affiliated to safe harbor-certified organizations.

The potential consequences of the Schrems decision together with the forthcoming General Data Protection Regulation, for the medicines and medical device sectors, with their increasing appreciation of the opportunities of using "Big Data" and being so U.S. dominated, are substantial. Three particular areas of current concern are the collection and processing of data from clinical trial and health technology assessment studies, pharmacovigilance and device vigilance (adverse event and incident reporting) and data on benefits given to health care professionals (increasingly required to be made publicly accessible by way of a central database or company website).

- In the case of research studies the critical issue is commonly ensuring that the patient consent form results in the consent being ‘informed’; sufficiently wide to cover primary and envisaged secondary uses; and covers data transfers outside the EU thereby hopefully obviating the need for safe harbor (or equivalent permitted data transfer options).

- With drug or device vigilance the absence of industry specific guidance has meant this is a grey area but the proposed General Data Protection Regulation clarifies that personal data can be processed without consent for the provision of care or treatment or the management of health care services reasons of public interest in the area of public health including ensuring high standards of quality and safety for medicines and devices.

Both the above issues also involve "pseudonymisation" techniques — replacing a name or other identifying elements by a code with the purpose of rendering the reidentification of the individual impossible or very difficult. This technique is viewed as privacy-enhancing rather than being effective to avoid data protection laws applying.

- In the case of benefits to health care professionals many companies seem to continue to use a form of implied or tacit consent, whereby health care professionals would be taken to have signified agreement by entering into an agreement with the pharmaceutical company or by continuing to work with the pharmaceutical company.

It is important to note that under the proposed new regulation, consent will have to be freely given, specific, informed and explicit. Consent cannot be inferred, it will need to be expressly given in advance of the transfer. In addition consent will not provide a legal basis for processing where there is a "significant imbalance between the position of the data subject and the controller." It seems possible that some clinical trials could fall within this definition and it therefore raises the question whether informed consent will continue to be sufficient in this context. This will narrow the circumstances where consent is valid compared to existing laws in many European countries. In any situation in which methods of obtaining consent or effective pseudonymisation are inapplicable or inadequate then transfer to the US could become yet more problematic as a consequence of this judgment.

—By Pulina Whitaker and Paul Ranson, Morgan Lewis & Bockius LLP

*Pulina Whitaker is a partner in Morgan Lewis' London office.*

*Paul Ranson is a consultant in Morgan Lewis' London office and has had in-house roles with GlaxoSmithKline and Merck Sharp & Dohme Corp. He is also legal adviser to the U.K. trade association for smaller and medium-sized companies and was a nonexecutive director of a specialty pharmaceutical company.*