Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Align APEC And EU Cross-Border Transfer Rules

Law360, New York (April 12, 2016, 3:10 PM ET) --


Hilary Wandall


Daniel Cooper

For most organizations, the ability to transfer data — including data that may relate to living individuals — across national borders is a self-evident business imperative. Companies engaged in international commerce must export data to affiliates, business partners, service providers, customers or employees for a variety of purposes: administering global IT systems, evaluating potential business opportunities, interacting with customers, managing the workforce, or complying with legal and regulatory requirements. New technologies, in turn, have emerged in recent years to help address this business need, such as cloud-based software applications and storage, e-commerce platforms and Internet-enabled mobile devices.

Just as business practices have evolved, legal frameworks regulating the processing of data have moved on as well, but in a notably different direction.[1] Most of these legal frameworks share common characteristics, such as rules requiring organizations to process data in an open and transparent manner, apply appropriate security measures to the data, refrain from amassing more data than necessary and delete or expunge data as soon as reasonably practicable. They nearly all contain restrictions on transferring data to another country or, in some cases, region, where the laws of that country or region do not provide for adequate or equivalent protections for the data. This poses a serious compliance challenge for companies conducting business on an international scale, given their need regularly to convey data to other countries.

In the absence of any commonly agreed criteria for deciding whether a country or region's data privacy protections are adequate, companies have found that their compliance strategies for exporting data out of one country cannot be readily transposed to another. This is a problem. That said, there now appear to be grounds for optimism. One multinational pharmaceutical company, Merck & Co. Inc., has demonstrated that it may be possible to square this compliance circle, to a degree, by implementing a data transfer compliance strategy that complies with the rules in both the Asia-Pacific Economic Cooperation[2] region and the EU.[3]

EU Privacy Framework

The European Union, today comprising 28 European member states, has long regulated the collection and transfer of personal data, enacting one of the first regional data protection statutes in 1995 with the

EU Framework Data Protection Directive 95/46/EC. The EU's efforts to regulate personal data inspired many other countries to enact comparable laws, although to date the European Commission only has designated a small number of foreign countries — Andorra, Argentina, Canada (for PIPEDA regulated entities), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey and New Zealand — as providing "adequate" protection for EU-originating data.

The United States has not been deemed to provide adequate protection, although the EU and the U.S. had negotiated a separate legal framework for trans-Atlantic data transfers, known as the "Safe Harbor." The Court of Justice of the European Union, in Case C-362/14 Maximillian Schrems v. Data Protection Commissioner, invalidated the Safe Harbor in October 2015, on various grounds, including that it was insufficiently protective of EU data. The U.S. and the EU Commission subsequently reached agreement on the terms of a new "Privacy Shield," announced on Feb. 2, 2016, which is not yet operational and is undergoing review by EU data protection authorities and a committee composed of representatives of the EU member states.

Companies thus attempting to transfer data from the EU to a nonadequate jurisdiction, such as the U.S., on a regular basis are required to comply with a limited set of compliance options, which practically speaking either involves obtaining individual consents, implementing commission-approved data transfer agreements (i.e., "model contracts") or adopting so-called binding corporate rules. BCRs have received strong support from the EU's data privacy regulators, which have published a number of guidance papers over the years to make it easier for industry to implement BCRs.

BCRs involve companies applying internal rules and procedures for their handling of personal data, which collectively ensure that the data are subjected to sufficiently robust privacy protections wherever they are sent in the organization, mirroring EU requirements. They are particularly favored where multinational companies wish to transfer data between and among their affiliates worldwide. Through this mechanism, companies can transfer their data internationally throughout the organization, provided the relevant company affiliates are both internally and externally bound to comply with the BCRs. This typically involves commitments reflected in internal policies, as well as the execution of a binding intra-group agreement.

BCRs are not easy to implement, however, as they require the company to participate in a complicated approval process involving discussions with a "lead" EU data protection regulator and two "backstop" regulators (together representing the interests of the other EU data privacy authorities).[4] These regulators evaluate the company's BCR application, recommend modifications and, ultimately, must approve the application. The BCR approval process can take a number of months to complete. Presently, 82 companies have successfully completed the BCR approval process.[5] Until recently, BCRs were not a transfer mechanism that resonated in other legal frameworks; it was viewed as a uniquely EU legal construct. Companies could rely on BCRs to move data from the EU, but they had less utility in transferring data from other non-EU countries.[6] As the Merck example demonstrates, this appears to now be changing.

APEC Privacy Framework

The APEC member states, for their part, have come to data privacy regulation more recently, but with vigor. A number of countries participating in APEC, including Australia, Canada, Chile, Hong Kong, Japan, Korea, New Zealand and Singapore, among others, have enacted data privacy laws. While less harmonized than the laws of the EU member states, these countries regulate international data transfers and impose conditions on their export, frequently requiring companies to impose a variety of

controls as diverse as those appearing in EU law.

In an attempt to encourage the free flow of data within the region, APEC member states endorsed an APEC privacy framework over a decade ago to set forth basic foundational principles for organizations processing data. The APEC cross-border privacy rules ("CBPR") system, which is a voluntary self-regulatory initiative designed to ensure the continued free flow of personal information across APEC member borders, emerged from this initiative in 2011. It relies upon approved "Accountability Agents," such as the U.S. company TRUSTe and the Japanese organization JIPDEC, verifying that an organization complies with CBPR program requirements on the basis of a CBPR "Intake Questionnaire" or a comparable assessment form completed by the CBPR applicant.

Where appropriate, accountability agents will assist the applicant in modifying its policies and practices to meet the requirements of the CBPR system. These include commitments, reflected in a company's internal policies and procedures, to abide by notice, collection limitation, choice, security, fair use, access and correction, and general accountability principles when receiving, processing and transferring data. There are currently four participating APEC member states — the U.S., Mexico, Japan and Canada, with additional countries expected to join in the future — and 13 companies with CBPR certifications.[7]

Aligning EU BCRs and APEC CBPR Certification

These efforts to align the cross-border data transfer rules within the EU and among APEC member states are laudable, but of limited utility where organizations have a business presence throughout the world and transfer data globally. Aligning requirements across, and not just within, the different regions would represent a watershed moment and be a welcome development for industry. Once achieved, businesses potentially would be in a position to apply a single set of internal policies and procedures to regulate their data transfers, regardless of where the data originated or where they were sent. In the absence of such alignment, companies may have no other choice but to adopt convoluted and complex privacy policies, which unrealistically seek to distinguish data based on their country of origin.

The omens are good that we are on the cusp of such a development. Experts representing the EU's Article 29 Working Party, comprised of EU member state data privacy regulators, and representing APEC member states commenced work in 2013 to produce a common reference work for organizations pursuing both EU BCRs and CBPR certification. It was commonly acknowledged that this would serve as a vital first step to establishing greater coordination in the regulation of cross-border data transfers in the two regions. If the two systems were to be made more compatible, then in theory it would be possible for a company to transfer data out of one region to the other relying on the same corporate policies and procedures. Published in 2014 by the Article 29 Working Party, the "Referential" served as a "pragmatic checklist" for organizations, setting out certain "common blocks" where the two systems overlapped and "additional blocks" where there were gaps.[8]

It was hoped that organizations would be able to leverage this checklist to develop a uniform set of corporate policies and procedures that complied both with the CBPR certification scheme and EU BCR requirements. Very few companies took up the challenge and were willing to serve as the first "test cases." However, on March 1, Merck became the first company to demonstrate that it can be done, by obtaining approval from European regulators for its EU BCR application, relying upon a global privacy program, including policies and procedures, that Merck previously had utilized to demonstrate compliance with the CBPR program requirements in seeking its initial CBPR certification in October 2013.

The Merck Example: A Marriage of Two Frameworks

The Merck example is significant because it shows that companies seeking to transfer data within the Asia-Pacific region, relying on a CBPR certification, and out of the EU, relying on a BCR application, are not forced to implement divergent policies and procedures. On the contrary, it now appears possible for companies to achieve dual certification and embrace the same privacy governance processes to comply with requirements imposed in both regions. The benefits for companies are clear: They can apply the same set of rules to their handling of data, which is plainly more attractive than having many sets of rules. It promotes more efficient internal handling of data, enables simplified privacy impact assessments, facilitates training and auditing exercises, lowers the attendant compliance risks, and avoids unnecessary delays and confusion.

Merck sought to adapt the documentation underpinning its CBPR certification to secure approval for a BCR application, rather than vice versa. This strategy appeared viable following an internal mapping exercise that the company conducted in late 2014, using the EU's BCR checklist in the Article 29 Working Party's guidance document, WP 153. As the EU "Referential" suggested and Merck's gap analysis confirmed, the company needed to supplement its existing policy documentation in certain respects, and make other commitments that included transforming its prioroutward facing privacy policies to create a novel fully-integrated publicly facing global cross-border privacy rules policy,[9] in order to satisfy the BCR criteria and to provide transparency for customers, regulators and other external constituents on the company's global data transfer practices across APEC, the European Economic Area and Switzerland. Merck made these adjustments, and was in a position to launch its application with its designated lead authority, the Belgian data privacy regulator, in late 2014. The U.K. and French regulators served as backstop authorities.

Merck's BCR application comprehensively referenced all manner of personal data, spanning clinical trial to employment data, transmitted by the company from the EU. Notwithstanding the expansive scope of the application, the company was able to proceed through the EU regulatory approval process more rapidly than normal and, while regulators requested some minor adjustments to the application materials, these were readily addressed without jeopardizing commitments made to achieve CBPR certification.

Ultimately, Merck was able to obtain its BCR approval on March 1, months ahead of schedule, and at remarkably lower cost than a traditional BCR application. It proved that dual CBPR and BCR can not only be accomplished, but that there are tangible benefits from adopting this strategy. Many companies now pondering their compliance strategies for data transfers should take note. Dual certification appears to be a real possibility and the Merck experience is likely to be a sign of things to come.

—By Hilary Wandall, Merck & Co. Inc., and Daniel Cooper, Covington & Burling LLP

Hilary Wandall is associate vice president, compliance and chief privacy officer at Merck & Co. Daniel Cooper is a partner in Covington & Burling's London office.

DISCLOSURE: Hilary Wandall led Merck's CBPR and BCR programs. Daniel Cooper is lead legal adviser on the Merck CBPR to BCR initiative.

[1] Over the past fifteen years, there has been an explosion of national and regional data privacy laws, which have led to greater controls on the processing of personal data, including its export. Once considered a European phenomenon, this is no longer the case. According to one recent estimate, well over 100 countries, including many in South and Central America, Asia and the Middle East, now have enacted data privacy laws, and many more are in the process of passing such legislation. Greenleaf, G. "Global data privacy laws 2015: 109 countries, with European laws now a minority" (2015). 133 Privacy Laws & Business International Report, February 2015.

[2] The Asia-Pacific Economic Cooperation ("APEC") group is an intergovernmental forum comprised of the 21 Pacific Rim member economies, focused primarily upon trade and economic issues, which has brought data privacy issues -- and its cross-border transfer -- into its remit. APEC's 21 Member Economies are the United States, Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Republic of Korea, Chinese Taipei, Thailand and Viet Nam.

[3] The European Union now comprises 28 individual member countries located primarily in Europe. These are: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[4] The so-called mutual recognition procedure is intended to expedite the approval process for BCRs. At the moment, 21 countries are part of the mutual recognition procedure : Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovakia, Slovenia, Spain, and the United Kingdom. The remaining EU Member State data privacy regulators participate in a "mutual cooperation" procedure, whereby they review -- generally on a fairly cursory basis -- the BCR application.

[5] A list of current BCR approved companies is available at: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

[6] Helpfully, a group of 15 francophone countries is developing a BCR mechanism that is expected to be aligned with the EU BCR model.

[7] A list of current CBPR certified companies is available at: https://cbprs.blob.core.windows.net/files/APEC%20CBPR%20Compliance%20Directory_Dec_11_2015.pdf.

[8] Article 29 Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents (adopted 27 February 2014).

[9] http://www.msd.com/privacy/cross-border-privacy-policy/