

Cross-Border Data Transfer Mechanisms

Center for Information Policy Leadership

August 2015

I. Introduction

Legislatures in many countries currently are drafting or amending data protection laws. Often, these drafts and amendments attempt to regulate cross-border data transfers by imposing restrictions on transfers of personal data to other countries that do not have similar data privacy laws. Sometimes they also include so-called data localization provisions that require data or copies of data to remain in the country of origin. Yet, global data flows are the product of the increasing globalization and digitalization of business processes and society and are foundational to the modern economy. The ability to use, share and access information across borders stimulates innovation, enables data-driven products and services and fuels economic growth and ideas, and is often the lifeline for remote communities. Any limitation on cross-border data flows, therefore, presents serious challenges to these key attributes and benefits of the global movement of data. This paper does not attempt to prove this particular point, however, as it has been discussed extensively elsewhere.¹ Instead, the paper enumerates important cross-border transfer mechanisms that should be included in any law that regulates or limits data transfers to other countries.

Initially, it should be noted that several significant countries with privacy laws, such as the United States, Canada, Mexico and Japan (prior to its proposed revision), do not impose material restrictions on cross-border transfers of personal information. From our perspective, these are not only viable but preferred models, particularly where organizations are required by legislation or jurisprudence to remain “accountable” for the continued protection of transferred data at the level it is protected inside the jurisdiction. Indeed, international privacy frameworks, such as the APEC Privacy Framework, also promote an approach based on accountability whereby the businesses need to exercise “due diligence and take reasonable steps” to ensure that the recipient organization will protect the information at the original level.

A different model based on the EU data protection laws, however, is proliferating around the world. Under that framework, countries prohibit cross-border data transfers to other countries whose privacy laws are not substantially similar to their own and thus deemed not “adequate”, unless certain specified derogations apply, or the transfers can occur under an exempted mechanism or recognized alternative transfer structures, which include concepts such as standard contractual clauses, binding corporate rules or safe harbor arrangements. Variations of this model containing differing selections of such derogations or mechanisms

¹ See, e.g., *Business Without Borders: The Importance of Cross-Border Data Flows to Global Prosperity*, US Chamber of Commerce and Hunton & Williams, 2014, available at https://www.huntonprivacyblog.com/files/2014/05/021384_BusinessWOBorders_final.pdf; see also *The Cost of Data Localization: Friendly Fire on Economic Recovery*, European Centre for International Political Economy (ECIPE), 2014, available at www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf.

can now be found in numerous laws, proposed laws and other legal guidance around the world, including in Malaysia, Singapore, Brazil and Hong Kong.²

Given this trend, it is essential that there be greater convergence between the specific ways countries approach the regulation of data transfers. Indeed, there is already a well-established body of precedents and best practices for data transfer mechanisms based on existing laws, regulatory guidance and organizational compliance programs. Moreover, global data flows and complex compliance strategies for the growing number of conflicting national requirements have become a key compliance priority for global organizations, and they have learned to deploy many and different mechanisms that enable the specific type of transfers and the particular jurisdictions involved. Accordingly, it is essential that countries legislating in this area take account of the existing and complex web of transfer mechanisms, laws and best practices that have evolved so that these mechanisms can work together and provide for seamless but still accountable global data flows that work for all kinds of cross-border data transfers, including transfers to or between controllers or processors and between affiliated companies or with third parties.

II. Data transfer mechanisms

We suggest that any legislator that has decided to include cross-border transfer restrictions in any data protection laws and regulations also include the following derogations, exceptions and alternative cross-border transfer mechanisms in such laws:

- 1. Contracts. The law should allow cross-border transfers on the basis of contractual arrangements that stipulate appropriate data privacy and security controls to be implemented by the organizations, thus establishing sufficient levels of protection for data leaving the jurisdiction.***

Contractual arrangements between transferors and transferees that establish legal obligations and the conditions under which data processing activities may take place are widely used by organizations globally, both for purposes of controller to controller transfers, and, even more frequently, controller to processor transfers. They are an effective means to ensure that the legal obligations that attach to the data continue to apply as the data moves between countries, thereby ensuring a high-level of protection of the data.

Because data flows occur within varying and specific business contexts, parties to a transaction must remain free to use contractual language that suits their specific business

² See Malaysia's Personal Data Protection Act of 2010, available at http://www.pdp.gov.my/images/LAWS_OF_MALAYSIA_PDPA.pdf; Singapore's Personal Data Protection Regulations 2014, available at <http://bit.ly/1wdBTMb>; Brazil's draft Law on the Processing of Personal Data, available at <http://pensando.mj.gov.br/dadospeessoais/english-information/>; Hong Kong's Personal Data (Privacy) Ordinance (transfer provisions not yet in effect), available at http://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html; see also EU Data Protection Directive of 1995, available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> (and the proposed EU General Data Protection Directive).

needs and information flows while also imposing the appropriate data privacy and security obligations applicable to the data. For example, the needs of businesses in the financial sector, health services sector, insurance sector, and advertising sector vary greatly and each have unique business and regulatory needs that are best handled by contractual provisions customized to their situations and their data handling needs. Indeed, this context-specific flexibility in contracting is essential and thus we strongly discourage an approach that requires parties to use non-modifiable standard contractual clauses for this purpose, as is currently the case with the EU standard contractual clauses³. Under that model, businesses are forced to have multiple contracts (one to meet their individual data processing needs and one merely to “tick-the-box” of privacy regulatory compliance), which is inefficient and ultimately does little to improve privacy protections. Rather, organizations should be able to adapt and tailor their contracts to the specific circumstances of the transfers to maximize both efficiency and privacy protections. This more flexible approach is evident in the privacy laws of countries such as Australia and Singapore.⁴

Finally, some laws include pre-approval requirements for such contracts. For reasons of efficiency and resource management, regulatory or governmental review and pre-approval of the contracts should not be required. It is sufficient that the data privacy regulators or individuals have the ability to challenge noncompliance with data transfer requirements through appropriate legal processes.

2. Corporate Rules. The law should allow cross-border transfers based on binding corporate rules.

Another important cross-border transfer mechanism are corporate rules. An example of this concept are the EU’s “binding corporate rules” (BCR).

Under that system, groups of corporate affiliates may transfer data to non-EU countries within their corporate group if the group has a set of rules, or BCR, that have been approved by a EU data protection authority. These BCR establish uniform internal rules for transferring personal data across the corporate group based on the EU data privacy requirements, and are binding on all relevant entities and personnel in the group. BCR exist both for organizations acting as controllers and as processors.

³ The EU “standard contractual clauses” for transfers between EU controllers and foreign controllers or foreign processors have been widely used by organizations doing business in or with Europe. However, the EU standard contractual clauses cannot be modified and must be used as published.

⁴ Office of the Australian Information Commissioner, Australian Privacy Principles guidelines, paragraph 8.16, available at http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP_guidelines_complete_version_1_April_2015.pdf; Singapore Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, paragraphs 19.2 to 19.6, available at [http://www.pdpc.gov.sg/docs/default-source/advisory-guidelines/the-transfer-limitation-obligation-\(chapter-19\).pdf?sfvrsn=0](http://www.pdpc.gov.sg/docs/default-source/advisory-guidelines/the-transfer-limitation-obligation-(chapter-19).pdf?sfvrsn=0).

BCR also require a compliance infrastructure, including governance mechanisms, data protection officers (DPOs), training and communication, audits and assessments and, in general, follow the essential elements of accountability and corporate compliance programs.⁵ Thus, corporate rules like the BCR are, in essence, an accountability mechanism. As such, they should be implemented more widely, especially in light of similar accountability mechanisms, such as the APEC Cross-Border Privacy Rules (CBPR), with which corporate rules could be made interoperable (see below).

To ensure wider uptake and scalability in the future, especially for SMEs, any corporate rules system should not require prior approval by a data protection authority. Instead, such corporate rules could either be self-certified or reviewed by a third-party “Accountability Agent” (see CBPR section below), as appropriate, and, with respect to government or regulatory oversight, companies that employ such corporate rules should stand ready to demonstrate their compliance on request.

3. Cross-Border Rules. The law should allow for enforceable corporate cross-border privacy rules modeled on the APEC Cross-Border Privacy Rules (CBPR).

We encourage the inclusion and recognition of cross-border transfer mechanisms such as the APEC CBPR developed by the Asia-Pacific Economic Cooperation (APEC) forum. The CBPR are an enforceable corporate code of conduct for intra- and inter-company cross-border data transfers that have been reviewed and certified by an approved third-party certification organization (“Accountability Agent”) in the jurisdiction in which the company is headquartered. Enforcement of the CBPR is provided by APEC data protection and privacy authorities that have joined the APEC Cross-border Privacy Enforcement Arrangement (CPEA). APEC is also in the process of implementing a corollary system for processors, the APEC Privacy Recognition for Processors (PRP).

The advantage of this system is that it allows transfers not only within a global corporate group (such as under the BCR), but also between unaffiliated companies and to companies that are not CBPR-certified anywhere in the world. The CBPR-certified company remains liable for the protection of the information at the level of the originating APEC country and the CBPR regardless of where the data is transferred.

Non-APEC countries that adopt similar mechanisms could make their cross-border rules mechanisms interoperable with the CBPR (and other similar schemes). This will have the effect of creating a global certification mechanism requiring only one approval process. Indeed, by way of exploring the viability of this approach, an effort is currently underway between APEC and the EU’s Article 29 Working Party to streamline the CBPR/BCR

⁵ For more information on the essential elements and types of accountability, see CIPL’s earlier white papers and materials on accountability, http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Data_Governance_Paper_2011.pdf; Canada’s “Getting Accountability Right with a Privacy Management Program” available at https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp; and Hong Kong’s Privacy Management Program, available at <https://www.pcpd.org.hk/pmp/pmp.html>

certification and approval processes when companies seek “dual certification” under both systems.

4. Codes of Conduct, Certifications, Privacy Marks, Seals and Standards. *The law should allow for the use of certified codes of conduct, certifications, privacy marks, and seals and standards as cross-border transfer mechanisms.*

Mechanisms related to corporate rules, BCR and CBPR, include codes of conduct, certifications, and privacy marks and seals (as envisioned by the EU Data Protection Directive and the proposed EU General Data Protection Regulation), and international standards, such as the ISO standards. All of these mechanisms also impose substantive privacy requirements on organizations and are externally certified and enforceable. Any privacy law with data transfer restrictions should allow for the use of such mechanisms to enable accountable cross-border data transfers, in the same way BCR and CBPR currently enable them.

5. “Safe Harbors” and Self-Certification Arrangements. *The law should allow the possibility of cross-border transfers based on negotiated safe harbor arrangements, including arrangements that rely on “self-certification” to a given privacy standard, coupled with enforcement.*

Privacy laws that have cross-border transfer restrictions should also retain the option to develop “safe harbor” frameworks and self-certification arrangements. The US/EU Safe Harbor Framework is one example. Under that framework, the US and EU negotiated a set of privacy principles for cross-border data transfers from the EU to the US to which US companies may “self-certify.” Once a company self-certifies to the Safe Harbor, compliance with these privacy principles becomes binding and enforceable. Developing variations of this bilateral accountability model should be an option under any privacy law that contains data transfer restrictions. It would provide relevant authorities the flexibility to create data transfer frameworks that are particularly suited for SMEs and for contexts in which third-party certification may be impracticable and unnecessary.

6. Consent. *The law should allow cross-border data transfers on the basis of the data subject’s consent.*

As is already the case under many laws, consent should remain one of the options for legitimizing data transfers to other countries. Of course, such consent should be limited to appropriate circumstances where obtaining prior consent is practicable and meaningful.

7. Adequacy and Whitelists. *The law should allow adequacy rulings and “whitelists.”*

A “whitelist” is a list of jurisdictions to which cross-border transfers have been pre-approved on the basis of that country’s privacy laws’ purported “adequacy” under the standards of the evaluating country. The EU pioneered this legal basis for data transfers, and it is gaining some ground in other jurisdictions. While we do not believe this is a particularly practical or effective way to deal with global data privacy challenges and data flows, these mechanisms may be useful in some contexts. Certainly, an individual assessment of the “adequacy” of

every other country's privacy regime is unrealistic and risks being immediately obsolete due to changing circumstances on the ground. Even if such a task were achievable and the necessary expertise and language skills available, the theoretical legal "adequacy" of a particular regime does not address issues such as actual compliance, enforcement, or enforceability in the evaluated jurisdictions. Nevertheless, where the relevant country assessments can be accomplished, "whitelists" and "adequacy" findings should be possible, provided that these transfer mechanisms are merely one of the many made available by law.

Similarly, such "whitelists" and "adequacy" findings could be applied to specific industries and sectoral laws in other countries, keeping in mind that the same issues remain in terms of these mechanisms' practicability and effectiveness as a broad solution to regulating and enabling global data flows. Nevertheless, with this caveat, this option should be available too, if it is one of many. Note that an example of a sectoral application of "adequacy" can be found in the proposed EU General Data Protection Regulation (GDPR). This option recognizes that specific industry or business sectors regulated by separate laws may be subject to privacy or data protection requirements that provide adequate protection for international data transfers from the perspective of the evaluating country.

8. Derogations and exceptions. *The law should include certain standard derogations that permit cross-border transfers. Data users should be able to rely on applicable derogations without prior regulator review or permission.*

Many privacy laws already include standard derogations or exceptions to their cross-border transfer restrictions. Some of the most frequently used derogations allow transfers where:

- the transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party and (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject;
- the transfer is for the purpose of legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is necessary for a legitimate interest of the controller or a third party that is not outweighed by the fundamental rights or freedoms of the data subject.

This list is not comprehensive and must include additional derogations. When drafting privacy legislation that contains transfer restrictions, it is advisable to make the list of derogations as inclusive and comprehensive as possible, taking into account, at a minimum, all derogations and exceptions that exist in comparable laws in other countries.

III. *Further Recommendation*

We specifically suggest that the following should *not* be included in provisions regulating cross-border data flows.

1. Notification and Registration. The law should not require that the Data Protection Authority be notified of a cross-border transfer, or that proposed categories of cross-border transfers be registered with or approved by the Data Protection Authority.

While, historically, some laws contain such requirements, the trend is moving away from this approach as it is cumbersome and does not enhance privacy compliance. Many countries now realize that these requirements do not add much to the actual protection of individuals on the ground. Also, given the prevalence and volume of global data flows, technology and processes, the enormous administrative burden and costs they impose both on organizations (especially SMEs) and on data protection authorities are not justifiable.

Summary

To conclude, if a legislature or regulator is to establish cross-border data transfer restrictions, it should also establish appropriate and effective exemptions so that necessary cross-border data transfers can continue while protecting the data and privacy of individuals. There are numerous available mechanisms and legal bases to facilitate such accountable transfers while still protecting individual privacy; and all of them should be included in any privacy law. Which one of them is appropriate for a given transfer scenario will depend on the context. Industry should be given flexibility in choosing which mechanism or legal basis works best under the circumstances and within the confines of appropriate accountability mechanisms and enforceability by the responsible authorities. Unnecessary government involvement should be avoided, as this imposes administrative and cost burdens on government and industry alike. Finally, accountability-based mechanisms that ensure effective and real protection for individuals, such as BCR, CBPR and similar mechanisms, should not only be an option, but specifically encouraged and incentivized.

For more information, please contact Bojana Bellamy, bbellamy@hunton.com, or Markus Heyder, mheyder@hunton.com.