Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy

CENTRE FOR INFORMATION POLICY LEADERSHIP WHITE PAPER

Bojana Bellamy
President

Markus Heyder
Vice President and Senior Policy Counselor

REVISED AND UPDATED EDITION
25 September 2017

2200 Pennsylvania Avenue
Washington DC 20037
202-955-1563

30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Park Atrium, Rue des Colonies 11
1000 Brussels
+32 (0)2 643 58 00

www.informationpolicycentre.com

EXECUTIVE SUMMARY

This white paper by the Centre for Information Policy Leadership (CIPL) is directed at all policymakers and legislators who are drafting privacy laws that regulate and contain restrictions for cross-border transfers of personal data.

While an approach to cross-border data transfers that relies on "accountability" for transferred data, rather than transfer restrictions, is both viable and preferable, an increasing number of countries are still including cross-border transfer restrictions modeled on the EU example. Given this trend, it becomes essential to ensure consistency and convergence and build on existing and accepted business and regulatory practices to enable benefits from cross-border data flows while ensuring protection from harms and risks for individuals. Therefore, privacy laws that do contain cross-border data transfer restrictions should also include the full range of existing and accepted exceptions and derogations to such restrictions, as well as a comprehensive set of available cross-border transfer mechanisms to enable accountable global data flows despite any transfer restrictions. These mechanisms include:

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.

2) Corporate Rules: The law should allow cross-border transfers based on binding corporate rules that provide for uniform and high-level protection and privacy compliance by all local entities of a multinational group.

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

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.

5) Self-Certification Arrangements: The law should allow the possibility of cross-border transfers based on negotiated arrangements, including arrangements that rely on "self-certification" to a given privacy standard, coupled with enforcement (such as EU-US Privacy Shield).

6) Consent: The law should allow cross-border data transfers on the basis of the data subject's consent.

7) Adequacy and Whitelists: The law should allow adequacy rulings and "whitelists."

8) Other grounds for transfer or derogations or exceptions to transfer restrictions, including: consent; necessity for the performance of a contract; public interest; establishment or defense of legal claims; vital interests; public register information; and legitimate interest.

Any derogations and exceptions to cross-border data transfer restrictions should be comprehensive in light of global practice.

Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy

A White Paper by the Center for Information Policy Leadership (CIPL)[1]
(Revised and Updated**)**

25 September 2017

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. They are foundational to the modern digital economy. The ability to use, share and access information across borders stimulates innovation, enables data-driven products and services, 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.[2] 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 and Mexico, 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 businesses need to exercise "due diligence and take reasonable steps" to ensure that information remains protected wherever it travels and that recipient organizations will protect information at the original level.

---

[1] CIPL is a privacy and data protection think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 54 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure effective privacy protections and the effective and responsible use of personal information in the modern information age. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

[2] *See,* e.g. *Business Without Borders: The Importance of Cross-Border Data Transfers 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 Costs of Data Localisation: 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.

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, cross-border privacy rules or bi- or multilateral cross-border transfer arrangements, such as the EU/US Privacy Shield Arrangement. Variations of this model containing differing selections of such derogations or mechanisms can now be found in numerous laws, proposed laws and other legal guidance around the world, including in Japan, Malaysia, Singapore, Brazil and Hong Kong.[3]

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 industry and regulatory 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

[3] *See* Japan's Act on the Protection of Personal Information, *available at* https://www.ppc.go.jp/en/legal/; 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/dadospessoais/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).

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 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 sector has 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 the parties to use non-modifiable standard contractual clauses for this purpose, as is currently the case with the EU standard contractual clauses.[4] 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 so long as they comply with and implement the relevant data protection requirements. This more flexible approach is evident in the privacy laws of countries such as Australia, Hong Kong and Singapore.[5]

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). BCR are not mentioned in the current EU Data Protection Directive, but were developed by the EU's Article 29 Working Party (WP29) as a cross-border transfer mechanism consistent with the Directive's requirements.

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

[4] 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. This will continue to be true under the EU General Data Protection Regulation (GDPR) that will come into effect on May 25, 2018.

[5] Australia Privacy Act 1988, Australian Privacy Principle 8, included in schedule 1 of the Privacy Act 1988, *available at* https://www.oaic.gov.au/privacy-law/privacy-act/; Hong Kong Privacy Ordinance, *available at* http://www.blis.gov.hk/blis_pdf.nsf/CurAllEngDoc/B4DF8B4125C4214D482575EF000EC5FF/$FILE/CAP_486_e_b5.pdf; Hong Kong Office of the Privacy Commissioner Guidance Note, *available at* https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf; Singapore Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, The Transfer Limitation Obligation (Chapter 19), paragraphs 19.2 to 19.6, *available at* https://www.pdpc.gov.sg/legislation-and-guidelines/advisory-guidelines/main-advisory-guidelines - AG1.

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. The EU GDPR, which will come into effect in May 2018, explicitly includes BCR and expands their potential application from use only within a corporate group to a group of enterprises "engaged in a joint economic activity."[6] The term "engaged in a joint activity" is not defined in the GDPR and could be interpreted broadly. However, regardless of the meaning in the EU context, ideally, the scope of application for any type of BCR should mirror that of the APEC Cross-Border Privacy Rules (CBPR) (*see* discussion below), which do not have "within-group" or "joint-economic-activity" limitations. In other words, it should be possible for two BCR-approved companies to share data between themselves, based on the fact that both have approved BCR and provide for an adequate and high level of privacy protection and a comprehensive privacy program.

BCR also require a comprehensive privacy program and compliance infrastructure, including governance mechanisms, data protection officers (DPOs), policies and procedures, training and communication, audits and assessments and, in general, follow the essential elements of accountability and corporate compliance programs.[7] Thus, corporate rules like the BCR are, in essence, an accountability mechanism, which ensures compliance with local law, as well as adequate protection for data transferred across borders. As such, they should be implemented more widely, especially in light of similar accountability mechanisms, such as the APEC 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 or 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 or certification mechanism for intra- and intercompany cross-border data transfers that have been reviewed and certified by an approved third-party certification organization

---

[6] *See* Art. 47(1)(a) GDPR.

[7] For more information on the essential elements and types of accountability, *see* CIPL white paper "Protecting Privacy in a World of Big Data, Paper 1, The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society," http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf; *see also* CIPL's earlier white papers and materials on accountability, http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_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.

(Accountability Agent) in the jurisdiction in which the company is headquartered. The CBPR's objective is to uphold privacy protections to the standard embodied in the APEC Privacy Framework, a statement of privacy norms endorsed by the APEC forum in 2005. 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 has also developed a corollary system for processors, called the APEC Privacy Recognition for Processors (PRP).

The advantage of this system is that it allows transfers not only within a global corporate group (or within a group of enterprises engaged in "joint economic activity") (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 or to whom 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) if and so long as there is substantial overlap in the data protection requirements within each system. This will have the effect of creating a global certification mechanism requiring only one approval process. Creating transfer mechanisms with global applicability would be a significant efficiency gain to multinational and global businesses, and would also help regulators and, ultimately, benefit individuals.

Importantly, by way of exploring the viability of this goal, an effort was started between APEC and the EU's WP29 in 2012 to streamline the CBPR/BCR certification and approval processes when companies seek "dual certification" under both systems. Now, with the enactment of the GDPR, this EU/APEC collaboration also includes the EU Commission and has broadened its exploration of interoperability with the CBPR to include not only EU BCR, but also, and possibly primarily, GDPR certifications and, down the road perhaps, GDPR codes of conduct. This effort to create interoperability could serve as a model for similar efforts between other regions and transfer mechanisms.

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, for example, by the EU Data Protection Directive and the EU GDPR), and international standards, such as the ISO standards. EU GDPR specifically encourages development of codes of conduct, certifications and seals and their use as data transfer mechanisms.

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 and as GDPR certifications and codes of conduct will in the future.[8]

[8] For a detailed discussion of certifications, see CIPL's white paper "Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms," April 2017, *available at* http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

5. ***<u>Bilateral or Multilateral Self-Certification Arrangements</u>. The law should allow the possibility of cross-border transfers based on negotiated bi- or multilateral arrangements, including arrangements that rely on "self-certification" to a given privacy standard, coupled with enforcement (such as EU/US Privacy Shield).***

Privacy laws that have cross-border transfer restrictions should also not preclude the option to develop bi- or multilateral frameworks and self-certification arrangements. The EU/US Privacy Shield 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 Privacy Shield, 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. ***<u>Consent</u>. 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 and individuals have a real choice. (*See also* Section 8 below.)

7. ***<u>Adequacy and Whitelists</u>. 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 (especially, given the long and onerous review process), 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 becoming 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 many available by law.

Similarly, such "whitelists" and "adequacy" findings could be applied to specific industries and sectoral laws in other countries (such as to transfers to processors, or outsourcing or cloud providers), 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 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. ***<u>Other Grounds for Transfer or Derogations and Exceptions</u>. The law should include other grounds for transfer or certain standard derogations or exceptions to data transfer restrictions that permit cross-border transfers. Data users should be able to rely on applicable derogations and exceptions 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 interest 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;
- 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;
- the data subject has consented to the transfer;
- the transfer is necessary for reasons of public interest;
- the transfer is necessary to protect the vital interests of the data subject or of other persons; and
- the transfer is made from a public register.

This list is not comprehensive and may include additional grounds, derogations or exceptions. When drafting privacy legislation that contains transfer restrictions, it is advisable to make the list of transfer grounds, derogations or exceptions as inclusive and comprehensive as possible, taking into account, at a minimum, all grounds, 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. ***<u>Notification, Registration and Pre-Approval of Data Flows</u>. The law should <u>not</u> 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 (including the EU GDPR), 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.

CROSS-BORDER DATA TRANSFER MECHANISMS

25 September 2017

2200 Pennsylvania Avenue
Washington DC 20037
202-955-1563

30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Park Atrium, Rue des Colonies 11
1000 Brussels
+32 (0)2 643 58 00

www.informationpolicycentre.com