APEC Policy Support Unit
POLICY BRIEF No. 23
October 2018

GDPR and CBPR: Reconciling Personal Data Protection and Trade

By María Vasquez Callo-Müller

I. Introduction

The entering into force of the European Union (EU) General Data Protection Regulation (GDPR) reminded everyone of the ubiquity of the use of personal data in our daily lives. The repercussions of the GDPR in the APEC region are of upmost importance. It imposes obligations on the collection, processing and transfer of personal data not only to businesses established in the European Economic Area (EEA)[1], but also to those not established in the EEA that provide goods or services to EEA residents or monitor their behavior. This new feature has immediate repercussions on businesses regardless of their size. Additionally, the GDPR applies to data processors, and brings other key changes in the form of new rights for data subjects (i.e. the right to be forgotten, the right of data portability) and new obligations for companies (e.g. designation of data protection officer, data breach notifications). Rules for transfers of personal data overseas are also incorporated.

Against this background, the relevance of personal data and the free movement of it, is important in terms of digital innovation and economic growth, both for traditional industries (automotive and finance, among others) as well as for typical digital businesses (e-commerce companies). As data-driven products and services can easily be rolled out across borders and reach new customer bases, the governance of personal data requires inevitably cross border approaches. This necessity will only increase with the widespread use of artificial intelligence since datasets are collected and stored across borders.

This policy brief examines two governance frameworks related to personal data protection: the GDPR, and the APEC Cross Border Privacy Rules (CBPR) system which operationalizes the APEC Privacy Framework, in order to find commonalities and differences, and importantly, to find ways to make them interoperable. The first section will start by situating the GDPR in context and explaining its most important features. The second section will provide a brief analysis of how the APEC CBPR system fits in the current global privacy landscape. The third section will provide a comparison of the two frameworks, and the fourth and last section will discuss the implications of the GDPR for companies in the APEC region.

II. General Data Protection Regulation (GDPR)

The GDPR[2] entered into force on May 25, 2018. It applies to data controllers (those who determine the purposes and the means for processing data) and processors (organizations that process personal data on behalf of the controller). The obligations contained in the GDPR have been characterized by many commentators as being too stringent. However, one positive aspect is that the GDPR is designed to lead to large-scale (although not full) harmonization of data protection laws across the EEA. In the long term, this will reduce the cost of compliance for companies. Yet, EEA members retain the ability to further legislate in certain areas, such as: employment law[3], designation of data protection officers[4], processing carried out in the public interest or in compliance with a legal obligation[5], and automated decision making and profiling[6].

[1] Since the GDPR was incorporated into the EEA Agreement by the EEA Joint Committee on July 6, 2018, the scope of the GDPR has extended to three of the four EFTA members (Iceland, Liechtenstein, and Norway) and 28 EU members, covering a total of 31 economies. Switzerland is not a party to the EEA Agreement.

[2] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1-88. As a Regulation, the GDPR does not need any implementation, being directly applicable and enforceable.

[3] GDPR art. 88.

[4] GDPR art. 37 para 1.

[5] GDPR recital 10.

[6] GDPR art. 22 para 2, subpara b).

1. GDPR's scope of application: Processing of personal data

The GDPR only applies to the processing (collection, use and disclosure) of personal data of an identified or identifiable person.[7] The GDPR also includes a broader definition of "special categories" of personal data that are subject to stricter rules. These categories include genetic data, biometric data, health data, data concerning a natural person's sex life or sexual orientation, and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership data. The processing of these types of data is in principle prohibited, except when the data subject has given explicit consent or the processing falls under specific statutory exceptions. Furthermore, EEA members can add more conditions to processing genetic, biometric or health data. In contrast, the processing of sensitive data is not uniform across the APEC region. Some APEC member economies include a definition of sensitive data in their data protection laws, while others do not.

2. GDPR's most important changes: Extraterritoriality and new rights and obligations

In comparison with the EU Directive 95/46/EC, the most important new features of the GDPR are the issues of the "extraterritorial" application and new rights and obligations.

(Extra) territorial application ("*European rules on European soil*")
On the one hand, the GDPR applies to controllers (and now to processors) "established" in the EEA. The concept of "establishment" is broad and flexible, being determined by: (i) a real and effective activity in the EEA region – even a minimal one, (ii) an activity exercised through stable arrangements, and (iii) personal data being processed in the context of that activity.[8]

On the other hand, the GDPR also applies even if the controller or processor is not established in the EEA, but processes data related to: (i) the offering of goods or services to data subjects in the EEA; or (ii) the monitoring of their behavior as far as their behavior take place within the EEA.[9]

Offering of goods or services: "Offering" does not require a payment to occur. The GDPR also covers services offered for free, such as social media services. Factors to consider when determining the offering of goods and services are, among others, the language or currency generally used in one or more EEA members (i.e. euros), and the mentioning of customers or users in the EEA.[10] In this context, the mere accessibility of a website in the EEA does not mean that a business necessarily intends to offer goods and services in that economy.

Monitoring of behavior: "Monitoring" refers to the tracking of a natural person on the internet, including potential subsequent use of personal data processing techniques to profile a natural person.[11] In this context, businesses in the APEC region will have to be aware of any web analytics tools (e.g. cookies) that track the behavior of EEA visitors to their sites.

New rights and obligations
New rights for data subjects are the right to erasure (commonly known as the right to be forgotten[12]), and the right of portability (which allows data subjects to request for the data that controllers hold about them and reuse it for their own purposes or provide it to another controller[13]).

The GDPR brings new obligations.[14] For the controllers, these include: implementing data protection by design and default; reporting data breaches to supervisory authorities within 72 hours, and when the data breach is of high risk to the rights and freedom, communicating it to the data subjects; carrying out data protection impact assessments; and keeping records of data processing activities, with the exception for companies with under 250 people when the processing is occasional, is not likely to result in a risk for the rights and freedom of individuals and does not involve a special category of data. As for the processors, the new obligations are: compliance with the instructions on processing

[7] The definition of personal data in the EU is quite broad. According to Article 29 Data Protection Working Party, personal data can be anything from a name, a photo, an email address, bank details, social media posts, medical information or even a computer IP address. See: Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data (WP 136). The GDPR does not apply to certain processing covered by the EU Law Enforcement Directive (Directive 2016/680/EC), processing for national security purposes and processing carried out by individuals purely for personal/household activities.

[8] Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, No. Case C-230/14 (CJEU October 1, 2015).
[9] GDPR art. 3. 2.
[10] GDPR recital 23.
[11] GDPR recital 24.
[12] The right to be forgotten applies when data is no longer necessary and consent is withdrawn. Exceptions to it include: the right of freedom of expression and information, when the EU law requires retention, and for the establishment, exercise or defence of legal claims. See: GDPR art. 17.
[13] GDPR art. 20.
[14] See: GDPR Chapter IV.

given by the controller; keeping records of processing activities; and notifying data breaches to the controller. Importantly, if the processor departs from the instructions given by the controller, it becomes itself a controller and therefore faces full compliance for its actions. For example, if a market research company deviates from the instructions from the controller (e.g. a travel company that collects data from customers), it will be directly liable for its actions and face full compliance with the GDPR.

Common obligations for the controller and processor are to designate a data protection officer; cooperate with the data protection authorities; and secure the processing of personal data (including by means of pseudonymization and encryption).

These new obligations will inevitably be translated into higher operational costs for businesses. Those costs involve hiring of new personnel (for example, data protection officers), acquisition of new technology, and seeking legal advice. According to Forbes, the appointment of a data protection officer can entail a salary between USD 71,000 and USD 354,000, depending on the size of the company. Furthermore, it is estimated that the U.S. Fortune 500 companies have spent roughly USD 7.8 billion in GDPR compliance. [15]

3. GDPR and cross border data flows

The GDPR provides that any transfer of personal data overseas (and "onward transfers"[16]) shall take place only if: (i) an adequacy decision was granted by the EU Commission to a third economy providing the same level of protection as in the EU [17]; (ii) appropriate safeguards are in place, including standard contractual clauses, binding corporate rules (BCRs), approved codes of conduct, and approved certification mechanisms; or (iii) certain derogations apply (e.g. consent).

Of the three, BCRs in particular are important for companies in the APEC region. In fact, to help companies applying for certification under the EU system of BCRs and the APEC Cross Border Privacy Rules (CBPR) system, a referential outlining the compliance and certification requirements of both systems was developed in 2014 by a working group consisting of experts from Article 29 Working Party of Data Protection Authorities in the EU and members from the APEC Electronic Commerce Steering Group's Data Privacy Subgroup. Although the referential is non-binding in nature, it could serve as a starting point for companies seeking certification in Europe and the APEC region. Building on the work related to CBPR-BCR interoperability and with the implementation of the GDPR, the Data Privacy Subgroup held a meeting with the European Commission in August 2017 to discuss issues on recognizing the CBPR system as a certification mechanism under the GDPR.[18]

III. APEC Cross Border Privacy Rules (CBPR) System

The CBPR system is a voluntary certification scheme that allows companies to transfer personal data (inter and intra company) in a safe manner across APEC economies taking part in the initiative.[19] As the APEC region is highly diverse, the CBPR is designed to be a very pragmatic instrument. In this sense, it reflects the institutional characteristics of APEC as a non-binding organization that encourages economic growth based on facilitated trade and investment. This allows the discussion of difficult issues in a safe environment, where the outcomes could find their way into pathfinders[20] as a starting point.

1. CBPR: A brief history

The first version of the APEC Privacy Framework of 2005 [21] conceptualized the CBPR as a "mechanism for 'mutual recognition' or 'acceptance' of different domestic privacy laws, which would allow for effective privacy protection without creating unnecessary barriers to cross-border information flows". [22] As the information

[15] Oliver Smith, "The GDPR Racket: Who's Making Money From This $9bn Business Shakedown," Forbes, May 2, 2018, https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/. See also: IAPP and EY, "IAPP EY Annual Privacy Governance Report 2017," accessed September 11, 2018, https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf.

[16] From an overseas economy to another overseas economy.

[17] At the moment, only a small group of economies outside the EU is found to provide adequate levels of data protection. Those economies are: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the U.S. The latest addition is Japan. Adequacy talks are ongoing with Korea.

[18] See: APEC, "Data Privacy Subgroup Meeting with European Union," https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Subgroup-Meeting-with-European-Union.

[19] Those economies are the US; Mexico; Japan; Canada; Korea; and Singapore.

[20] A pathfinder is a cooperative project among participating APEC member economies.

[21] Born during the e-commerce boom, the first version of the APEC Privacy Framework traced its origins to 1998 when APEC Ministers agreed on a Blueprint for Action on Electronic Commerce, that recognized the necessity "to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy (…)." This recognition led to the development of the APEC Privacy Framework, which was formally endorsed by APEC Ministers in 2004.

[22] Section III on Cooperative Development of Cross Border Privacy Rules, APEC Privacy Framework, version 2005, p. 36.

privacy principles contained in the APEC Privacy Framework only apply to the data controllers, the CBPR likewise applies to the controllers of personal information (i.e. information about an identified or identifiable individual). In comparison with other international instruments such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines), the APEC Privacy Framework explicitly intended to reconcile personal data protection and trade.

Based upon further work by the APEC Electronic Commerce Steering Group and the APEC Data Privacy Pathfinder of 2007[24], the CBPR was finally endorsed in November 2011. In 2012, the U.S. became the first member economy to take part in the CBPR system. In August 2012, IBM became the first company to be CBPR certified. Furthermore, in order to align with the updated OECD Guidelines of 2013, the APEC Privacy Framework was updated in 2015.

Currently, the trend worldwide is to intensify the level of regulations for the processing and transfer of personal data. In this context, it makes good business sense, even in APEC economies with no data protection laws in place, to adopt minimum standards such as those included in the APEC Privacy Framework. Businesses preparing for international markets should at least implement businesses models and processes in light of the requirements of the CBPR. However, economies in the APEC region should be aware that domestic data protection laws in other jurisdictions (e.g. GDPR) could exceed those minimum standards.

2. CBPR: Who can take part?

The CBPR works at two levels: (i) APEC member economy, and (ii) the company. The same logic applies to the Privacy Recognition for Processors (PRP) system which was endorsed in 2015.[25] The following provides a general overview of the application process.

Table 1. CBPR Application Process

APEC Member Economy	Company
Step I. Self-assessment/Submission of relevant documents	
-Confirmation of participation in the APEC Cross Border Privacy Enforcement Arrangement (CPEA), with at least one Privacy Enforcement Authority. -Confirmation of intention to use at least one of the APEC-certified Accountability Agents. -Details of domestic laws for the protection of personal information and mechanisms for enforcement. **In the case of the PRP system, there is no requirement to be part of the CPEA.*	-Selection of Accountability Agent. -Self-assessment of compliance with APEC Privacy Framework principles. -Filling up intake questionnaire. **As the APEC Privacy Framework principles only apply to controllers, processors are not bound to demonstrate compliance with them.*
Step II. Compliance/Review	
Evaluation by Joint Oversight Panel and submission of report to Chair of Electronic Commerce Steering Group.	Evaluation by Accountability Agent.
Step III. Recognition/Acceptance	
Approval notification to APEC member economy by Chair of Electronic Commerce Steering Group.	Inclusion of applicant in compliance directory.
Step IV. Compliance/Enforcement	
Joint Oversight Panel may terminate or suspend the participation of an APEC member economy.[23]	Enforcement through Privacy Enforcement Authority and Accountability Agent. **In the case of the PRP system, enforcement actions occur via the controller (principle of accountability). Other forms of oversight and enforcement may exist at the domestic level.*

Source: Author's elaboration of the CBPR application process.

[23] See: Charter of the APEC Cross Border Privacy Rules System Joint Oversight Panel, section 5.

[24] The APEC Data Privacy Pathfinder was established by Ministers in 2007 to enable participating APEC member economies to work together to develop a framework for accountable flows of personal data across the region.

[25] The PRP system is a certification mechanism for data processors to demonstrate their ability to provide effective implementation of a personal information controller's privacy obligations related to the processing of personal information. The PRP system also helps controllers to identify qualified and accountable processors.

One of the main challenges of the CBPR system is the low number of Accountability Agents. While the existence of an Accountability Agent in each applying economy is not a requirement to be part of the CBPR, it is essential for ensuring accountability in the system. This aspect has proven to be a challenge as currently there are only two APEC-certified Accountability Agents (i.e. TRUSTe in the U.S. and JIPDEC in Japan).

3. CBPR as a certification mechanism: How it works and interoperates with other privacy frameworks?

The CBPR essentially certifies that a company complies with the APEC Privacy Framework, which is composed of four parts: (i) preamble and objectives, (ii) scope and coverage, (iii) nine information privacy principles, and (iv) domestic and international implementation.

The nine APEC information privacy principles (accountability; notice; choice; collection limitation; integrity of personal information; uses of personal information; security safeguards; access and correction; and preventing harm) resemble to a large extent the OECD principles for data processing as contained in the 2013 OECD Guidelines. On the other hand, an analysis of the nine APEC information privacy principles against the six GDPR principles for data processing (accountability; lawfulness, fairness and transparency; accuracy; purpose limitation; integrity and confidentiality; and storage limitation) reveals overlapping areas.

For instance, the APEC information privacy principles of "notice", "choice" and "collection limitation" are similar to the GDPR principles of "lawfulness, fairness and transparency". The APEC information privacy principle of "preventing harm" requires the notification of significant data breaches to Privacy Enforcement Authorities, which is in line with the "accountability" principle found in the GDPR. In other cases, the GDPR contains principles that go beyond the privacy principles contained in the OECD Guidelines or the APEC Privacy Framework. This is the case of the GDPR data processing principle of "accuracy" which is only partially reflected in the APEC information privacy principle of "integrity of personal information", except for the obligation of the controllers to erase or rectify inaccurate data without delay. The one GDPR principle with apparently no counterpart among the APEC information privacy principles is the principle of "storage limitation", which requires not keeping data for longer than necessary.

It has been argued that the CBPR would fall below more stringent domestic privacy laws.[26] However, this is misleading. The CBPR does not interfere with the ability of an economy to impose higher data privacy standards. Moreover, a review of the implementation of the APEC Privacy Framework at the domestic and international levels reveals certain level of interoperability with the OECD and GDPR frameworks. For instance, the updated OECD Guidelines of 2013 and the APEC Privacy Framework of 2015 incorporate new concepts, such as privacy management programs, security breach notification, national privacy strategies, education and awareness, and global interoperability. Furthermore, the CBPR intake questionnaire for APEC member economies and companies reiterates the importance of aspects found in the GDPR. This is the case of the appointment of a data protection officer. A comparison of the common elements across the OECD, APEC and GDPR frameworks at the implementation level is presented below.

[26] Griffin Murray, "Aussie Move to Join Asia-Pacific Privacy Plan Gets Mixed Reviews," Bloomberg News, December 1, 2017, https://www.bna.com/aussie-move-join-n73014472702/.

Table 2. Interoperability of the OECD, APEC and EU Privacy Regimes: Domestic Implementation

OECD (2013)	APEC Privacy Framework (2015) & CBPR	GDPR (2016)
Development of domestic privacy strategies		
Included.	Not mentioned as the Framework does not override domestic law.	Not applicable as regulation applies directly to EU members.
Adoption of laws protecting privacy		
Included.	Not mentioned.[27]	Only in cases of special categories of personal data.
Establishment of privacy enforcement authorities		
Included.	Included along with other forms of enforcement.	Included (Domestic Supervisory Authority).
Promotion of self-regulation		
Included.	The CBPR is itself an instrument of self-regulation.	Included. Can take the form of binding corporate rules (BCR), codes of conduct, etc.
Reasonable means for individuals to exercise their rights		
Included.	Included.[28]	Included.[29]
Provision of adequate sanction		
Included.	No specified.	Included.[30]
Adoption of complementary measures (e.g. education, awareness raising)		
Included.	Included.	Included.
Consideration of actors other than controllers		
Included.	Included (e.g. Privacy Recognition for Processors (PRP) system).	Applies to controllers and processors.
Exceptions for sovereignty, domestic security and public policy		
Allowed.	Allowed.	Allowed.
Implementation of privacy management programs		
Included.	Included.	Included (Data protection policies).
Cooperation within and between the public and privacy sectors		
-	Included.	-

Source: Author's elaboration

Table 3. Interoperability of the OECD, APEC and EU Privacy Regimes: International Implementation

OECD (2013)	APEC Privacy Framework (2015)	GDPR (2016)
Development of metrics		
Encouraged.	Encouraged.	-
Cross border cooperation		
Encouraged (e.g. information sharing).	Operationalized via APEC Cross Border Privacy Enforcement Arrangement (CPEA).	Supervisory authorities in charge of cross border cooperation, mutual assistance, exchange of information.
Operationalization of principles for data transfers		
Promotion of mechanisms.	CBPR, Privacy Recognition for Processors (PRP) system.	Binding corporate rules (BCR), among others.
Data cross border transfers		
Allowed subject to the observance of OECD guidelines or when there are sufficient safeguards in place. Restrictions should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.	Should not be blocked when member economy is party to CBPR or sufficient safeguards exists. Restrictions should be proportionate to risks. Onward transfers not mentioned (Principle of accountability applies).	Allowed subject to adequacy decisions, appropriate safeguards, or GDPR derogations. Onward transfers subject to the same conditions.
Promotion of interoperability		
Encouraged.	Encouraged.	-

Source: Author's elaboration

[27] However, when reviewing domestic privacy protection, take all reasonable steps to remove unnecessary barriers for information flows and to avoid creating such barriers.
[28] The CBPR contains mechanism for individuals to exercise their rights via Accountability Agents and Privacy Enforcement Authorities.
[29] This is a very important aspect of the GDPR. Individuals can: lodge complaints against a single supervisory authority, ask a non-profit organization or association to lodge a complaint on its behalf, and bring actions for annulment of decisions of the EU Data Protection Board against the Court of Justice of the EU.
[30] Monetary sanctions can amount to up to 20 million euros or 4 percent of annual global turnover, whichever is higher. Some EU members can impose criminal sanctions.

IV. A comparative look at CBRP, OECD Guidelines and GDPR

1. Partial overlapping

As the tables above show, the APEC Privacy Framework and the CBPR partially align with the GDPR and the OECD Guidelines as they include concepts such as the Privacy Enforcement Authorities, privacy management programs, and promotion of technical measures to protect privacy. The international implementation of the APEC Privacy Framework is also worth highlighting. It puts forward information sharing among member economies, cross border cooperation in investigation and enforcement, cross border transfers of data, and interoperability between privacy frameworks.

The GDPR on the other hand, includes principles and obligations that are not covered by the APEC Privacy Framework, the CBPR or the Privacy Recognition for Processes (PRP) system. The principle of "storage limitation" found in the GDPR does not appear to be reflected in the current APEC Privacy Framework. As for the obligations, gaps are found with regard to mandatory data breach notifications[31], restrictions for automated processing and profiling, handling of special personal information, and onward transfers. The direct application of some those obligations to the processors is also an aspect that differs from the CBPR.

2. Enforcement

Enforcement actions have not yet occurred for the GDPR. It is unclear how cross border enforcement will work. In the case of the CBPR, enforcement actions take place essentially at the domestic level. [32] However, the CBPR ecosystem also includes the APEC Cross Border Privacy Enforcement Arrangement (CPEA), as a multilateral arrangement that provides the first mechanism in the APEC region for Privacy Enforcement Authorities to voluntarily share information and provide assistance for cross border data privacy enforcement. The CPEA could be considered as a good practice in global personal data governance frameworks as it helps to ensure data protection compliance across borders while boosting consumer confidence. The CPEA also aligns well with other global initiatives such as the Global Privacy Enforcement Network which was formed in response to an OECD recommendation.

3. Contrasting governance models

The GDPR is a detailed regulation that works "top-down". It prescribes a series of obligations that should be met by companies and imposes hefty fines if those are not met. In contrast, the CBPR is a model of self-regulation. Furthermore, except for the intake questionnaire that an APEC member economy should fill up in order to submit its application to the Joint Oversight Panel, the CBPR is not prescriptive in the details and does not mandate how an economy should modify its data privacy laws. Instead, the CBPR system works "bottom-up" towards a facilitated global data governance, which at the same time facilitates data sharing and reuse. The CBPR is a good example of promoting global interoperability of privacy regimes based on minimum standards. As more member economies and companies join the system, the CBPR could become an effective mechanism for privacy protection that works towards the avoidance of barriers to information flow, and ensures continuous trade and economic growth.

4. Personal data protection and trade

Personal data (and the free flow of it) will be the cornerstone of digital innovation and economic growth in the coming years. Given that its regulation differs across the world and due to societal perceptions, it is necessary to find mechanisms that will allow for meaningful data protection laws at the domestic level and the adequate use of it by businesses at the international level. Those mechanisms are not easy to find. It has been suggested to include data protection negotiations in trade talks, but this is difficult for many reasons. First, in some cases, privacy and personal data are fundamental rights and therefore prevail over any other consideration, including trade.[33] Second, there are "differences in perceptions of the degree to which interests that compete with privacy, such as public safety and domestic security, warrant protection at the expense of privacy interests." [34] On top of that, emergent cybersecurity laws restrict cross border data flows by requiring data to be stored on shore. The following figure depicts how restrictions to cross border data flows have evolved over time.

---

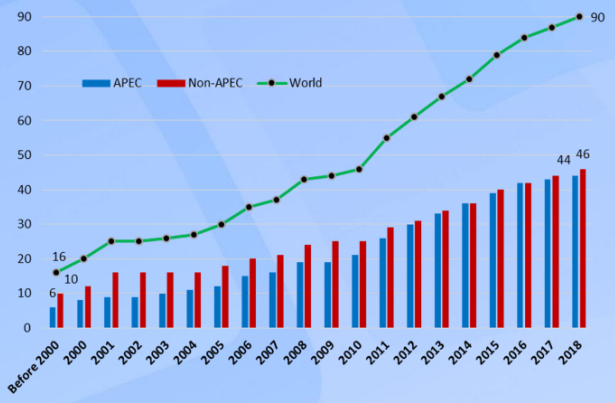
[31] In the APEC Privacy Framework, the notification of significant data breaches is encouraged (as a way to implement the "preventing harm" principle). However, this is not mandatory.

[32] The Federal Trade Commission already undertook enforcement action against the U.S. companies for deceiving consumers about their participation in the APEC CBPR system. See: "FTC Approves Final Order in Vipvape APEC Cross Border Privacy Rule Case," *The Computer & Internet Lawyer*, January 9, 2016. See also: https://www.ftc.gov/news-events/press-releases/2017/04/ftc-approves-final-orders-resolving-allegations-companies?utm_source=govdelivery.

[33] This was recently pointed out during the conclusion of the EU-Japan Free Trade Agreement.

[34] Bygrave, "Privacy and Data Protection in an International Perspective," 177.

Figure 1. Cumulative Number of Restrictions on Cross Border Data Flows



Source: APEC Secretariat, Policy Support Unit calculations, based on European Centre for International Political Economy (ECIPE), Digital Trade Estimates Database.

Finally, even in long established e-commerce issues, there are still divergences among several parties on how to carry on further negotiations, which would make any discussion about free cross border data flows unlikely to happen (anytime soon) in multilateral forums such as the WTO. In this context, scenarios such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the U.S.-Korea Free Trade Agreement, which contain a provision for the cross border flow of personal data within their e-commerce chapters, are rare and exceptional. Yet, as more CPTPP signatories are expected to ratify the trade agreement, momentum to include provisions facilitating cross border data flows could occur. Furthermore, there are other mechanisms to balance trade objectives with personal data protection such as the CBPR system.

V. Final Remarks

Some important conclusions can be drawn from this policy brief.

Extraterritorial reach of the GDPR: Companies in the APEC region that depend on personal data but are not "established" in the EEA will be captured by the GDPR if they either target the offerings of goods or services to, or monitor the behavior of, individuals in the EEA. This could be the case of e-commerce companies, websites or apps offering goods or services to individuals within the EEA. Furthermore, data controllers and processors not based in the EU, but covered by the GDPR, will have to appoint a data protection officer and in some cases a representative in the EU (exceptions apply as contained in art. 27 of the GDPR). Additionally, data processors such as payroll companies, providers of IT solutions, and data analytics face direct obligations under the GDPR.

Cross border data flows: Only four APEC member economies have received an adequacy decision from the European Commission, namely: Canada; New Zealand; the U.S.; and Japan[35]. This means they have been determined as having an adequate level of data protection for data transfers overseas. For other member economies, the pursuit of an adequacy decision by the EU can entail significant burden. Therefore, further work on the interoperability of the CBPR system and the adequate safeguards included in the GDPR could benefit companies in the region in the long term as it would enable cross border data flows. Meanwhile, member economies may still find their own way on the governance of personal data protection.

Outlook for the CBPR: The CBPR establishes bottom line standards for personal data protection to facilitate cross border personal data flows. Yet, in light of the GDPR, there are a few aspects that should be considered while constructing bridges for interoperability. Some of those are the principle of storage limitation; obligations regarding onward transfers, processing of special data, data breach notifications; the rights to be forgotten and of data portability; and importantly, enforcement actions against processors. A good practice to spotlight is the CPEA and the overall governance approach of the CBPR, which will allow APEC member economies to decide for themselves their domestic levels of personal data protection while facilitating trade and investment in the region.

[35] Alongside the EU-Japan Free Trade Agreement concluded in July 2018, the EU and Japan also agreed on a reciprocal adequacy decision for cross border data flows. Therefore, the data protection laws of both jurisdictions are deemed to offer comparable levels of protection. See: EU Commission Press Release "Questions & Answers on the Japan adequacy decision," July 17, 2018, http://europa.eu/rapid/press-release_MEMO-18-4503_en.htm.

María Vasquez Callo-Müller is the 2018 Google Policy Fellow at the APEC Policy Support Unit and Doctoral candidate at the World Trade Institute, University of Bern, Switzerland. The author would like to thank Dr Denis Hew, Carlos Kuriyama and Aveline Low for their valuable comments on earlier drafts. The author can be contacted at Maria.Vasquez@wti.org.

APEC Policy Support Unit (PSU) is the policy research and analysis arm for APEC. It supports APEC members and fora in improving the quality of their deliberations and decisions and promoting policies that support the achievement of APEC's goals by providing objective and high quality research, analytical capacity and policy support capability.

Address: 35 Heng Mui Keng Terrace, Singapore 119616
Website: www.apec.org/About-Us/Policy-Support-Unit
E-mail: psugroup@apec.org

APEC#218-SE-01.10