TOWARDS A TRULY GLOBAL FRAMEWORK FOR PERSONAL INFORMATION TRANSFERS

COMPARISON AND ASSESSMENT OF EU BCR AND APEC CBPR SYSTEMS

SEPTEMBER 2013

ACKNOWLEDGEMENT

Funding for this paper was provided by Google Inc. All opinions contained in this paper reflect the independent views and analysis of Information Integrity Solutions Pty Ltd.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

Today, digital innovations and breakthroughs transcend national boundaries. A truly global framework for the safe and efficient transfer of personal information across borders is needed for businesses and economies to realise the full potential of the data-driven environment while maintaining consumer trust. This report considers the European Union's (EU) Binding Corporate Rules (BCR) and the Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules (CBPR) System, two regional approaches that enable companies to engage in low friction cross-border transfers of personal information.

A side-by-side comparison of BCR and CBPR demonstrates that they are substantially similar in their participation criteria, both in terms of the underlying privacy principles and the content of the rules themselves such as the requirement for privacy staff, privacy training, complaint handling and independent assurance of compliance. These similarities will help facilitate future cooperation between the two systems.

The report also finds that operationally, BCR and CBPR take slightly different pathways to achieve the same result of providing protection for individuals while facilitating the efficient transfer of personal information across borders. Each system contains useful components that could inform the development of a global framework for international transfers.

As the first cross-border system of its kind, BCR is built upon important concepts such as:

- The centrality for data subjects' rights to be respected and enforced regardless of where their data is transferred
- The notion that corporate rules must be binding both internally (relating to compliance in practice) and externally (relating to legal enforceability)
- The designation of a single corporate member to take responsibility when something goes wrong.

The CBPR System, currently being implemented, has several advantages including:

- Enabling low friction transfers between different companies in participating APEC Economies, thereby extending beyond the scope of BCR's intra-group transfers
- The emphasis on cross-border regulatory cooperation, including both formal arrangements and operational requirements
- The use of Accountability Agents complements the role of Privacy Enforcement Authorities and enhances privacy protection by increasing the system's overall capacity to monitor compliance, address complaints and allow the Authorities to focus on serious breaches of privacy elsewhere.

The CBPR System contains parallels to the longstanding financial information governance framework, in particular through the introduction of independent third-party Accountability Agents.

A global governance framework for the safe and efficient transfer of personal information across borders represents a logical next step given the rise of personal information as a valuable asset class.

2 DESCRIPTION

2.1 INTRODUCTION

Global interconnectedness and the rise of personal information as a valuable asset have combined to make international transfers of personal information more important to companies than ever before. As with any asset, it needs to be managed, protected and surrounded by a suitable governance framework.

At the same time, privacy and respect for individuals have become key issues in the digital age. Privacy laws have proliferated around the world, albeit with varying degrees of consistency between jurisdictions.

Cognisant of these realities, for the past decade governments and industries around the world have increased their effort to find ways to facilitate international transfers that promote commerce and protect personal information. To date, the effort has been focused on the private sector rather than government agencies.

Two major geopolitical bodies – the EU and APEC – have developed their own regional frameworks.

The EU's BCR allows companies with a presence in the EU to transfer personal information to and from corporate members located outside of the EU, subject to Directive 95/46/EC (the Data Protection Directive). APEC's CBPR System, currently being implemented, will allow CBPR-certified companies in participating Economies to transfer personal information to each other subject to the APEC Privacy Framework.

Incremental steps are being taken to move beyond a regional approach. The EU's Article 29 Working Party and the APEC Data Privacy Subgroup are undertaking initial work to promote cooperation between the two systems.

This report complements these efforts by considering BCR and CBPR in light of moving towards a truly global framework. Rather than starting from a blank slate, the two systems provide useful insights into any such developments and will be important building blocks. The analysis is conducted with an emphasis on the business perspective.

2.2 THE PURPOSE OF A FRAMEWORK FOR PERSONAL INFORMATION TRANSFERS ACROSS BORDERS

In order for individuals to be comfortable with personal information about them moving between jurisdictions, they expect that the level of protection of that information will not diminish simply because of the transfer, both in terms of the level of protection and their enforcement. Companies that engage in such transfers are seeking to ensure that any frameworks achieve their objective with minimum friction.

Both BCR and CBPR are aimed at facilitating low friction cross-border transfers while ensuring that whatever protection the data has at the place of origin is maintained at the destination. As described below, they accomplish this in broadly similar ways.

2.3 BCR EXPLAINED

2.3.1 BACKGROUND

The EU Data Protection Directive places restrictions on the transfer of personal data about Europeans to entities and jurisdictions outside of the EU, as part of a framework to provide them with suitable data protection. Such transfers are allowed if the transfer is to a jurisdiction that has satisfied the EU that it provides an adequate level of privacy protection (Article 25). So far only a handful of jurisdictions have done so.[1]

The Directive also provides a number of derogations (exceptions) to the requirement for jurisdictions to satisfy the EU about the adequacy of privacy protection they offer, contained in Articles 26(1) and 26(2). Article 26(2) states that a Member State may authorise transfer of personal data to a third country where the sender can adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of the data subjects. Examples include:

- Appropriate contractual clauses
- Participation in the US-EU Safe Harbour Framework
- Binding Corporate Rules.

Article 26(1) contains derogations that do not require prior authorisation or the demonstration of adequate safeguards, such as:

- The data subject has given free, informed and unambiguous consent
- The transfer is necessary for the performance of a contract between the sender and third party concluded in the interest of the data subject
- The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.

The Article 29 Working Party recommends that the derogations in Article 26(1) are to be interpreted strictly and should only be used if it is not appropriate or possible to rely on Article 26(2).[2]

Companies wishing to transfer data routinely out of the EU can use contractual clauses that provide adequate safeguards for protecting the rights of European data subjects. The European Commission has drafted a set of standard contractual clauses for commercial use pursuant to Article 26(4).

For companies engaged in extensive data transfers both within and outside of the EU, contractual documents pertaining to only a defined set of transfers are often impractical for their business needs. This approach may lead to the company having to manage, monitor and keep up-to-date hundreds or thousands of contracts.

[1] European Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries' (11 February 2013) <http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm>.

[2] Article 29 Data Protection Working Party, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (25 November 2005) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf>

In recognition of this problem, the EU has introduced Binding Corporate Rules pursuant to Article 26(2) that:

- Are internal rules adopted by a company which define its global policy with respect to the transfer and handling of personal data within the same group
- Are internally binding on all employees and externally binding on all group members via enforcement by data subjects, including through the Data Protection Authorities (DPAs) and the courts
- Provide for privacy protection in line with the principles contained in the Data Protection Directive
- Provide for processes to ensure effective privacy protection, including training, complaint handling, audit and creation of a network of privacy officers/staff.

2.3.2 OPERATION

Each set of BCRs is tailor-made for the particular company in question. An application is submitted to the DPA of the corporate group's EU headquarters or group member with delegated data protection responsibilities. The lead authority circulates the rules to the other DPAs in EU countries where group members are located. Once the BCR is considered final by all relevant DPAs, the company can request authorisation of transfers by the relevant Member States pursuant to the Article 26(2) derogation.

The result is a collection of self-contained, self-governing arrangements for each company. Under its BCR, a company can send personal data to any jurisdiction in the world, as long as the receiving party is a member of the same corporate group, and each party is compliant with the Data Protection Directive. This ensures that the data receive the same protection wherever it goes.

For example, Hewlett Packard (HP) is able to transfer the personal data of its European employees and customers to other members of the worldwide group of HP companies. However, members of the HP group in the EU cannot send personal data to Intel entities located outside the EU, even if both companies have their own BCRs.

Meanwhile, transfers within the EU – for example between HP entities or from HP to Intel – are already covered by the Data Protection Directive and do not require BCRs.

2.3.2.1 CONTROLLERS VS PROCESSORS

The Data Protection Directive distinguishes between data 'controllers' and 'processors'. A data controller is a natural or legal person or other body that determines, alone or jointly with others, the purposes and means of the processing of personal data (Article 2(d)). A data processor is a natural or legal person or other body which processes personal data on behalf of the controller (Article 2(e)). The characterisation depends on the activities of an entity in a specific context – an entity may be a controller in certain situations and a processor for others.

The designation of controller or processor plays a crucial role in the application of the Directive and the exercise of data subjects' rights. Controllers have the greater responsibility of complying with the full suite of data protection requirements because they collect the personal data and decide what to

do with it. Processors are responsible for processing the data in accordance with instructions and to keep the data secure.

When first proposed in 2003, BCR applied only to data controllers. With the growth of cloud computing services since that time, the outsourcing of data processing and storage has become an increasingly indispensable part of global business. In light of this, BCR for data processors was launched on 1 January 2013. The application criteria are substantially similar, with some increased obligations to cooperate with the relevant data controller and the Data Protection Authority responsible for that data controller.[3]

BCR for data processors allows personal data to be transferred by processors to sub-processors in the same corporate group.

Where a BCR controller or processor wishes to sub-process personal data using a foreign entity outside of the corporate group, the adequacy or contractual route will ordinarily apply.

2.4 CBPR EXPLAINED

2.4.1 BACKGROUND

The 21 Economies that comprise APEC have great political, legal and developmental differences. Some Economies like Australia, Canada, Japan, Mexico, New Zealand and Singapore have comprehensive privacy legislation while others do not, such as China and Indonesia. Many Economies have privacy laws that apply only in particular circumstances, including the United States of America. This raises the familiar problem of how privacy protection for individuals will be guaranteed when personal information is transferred between Economies with such a variety of laws in place.

APEC began to address this in 2004 when the Economies endorsed the APEC Privacy Framework to promote the free flow of personal information across borders while establishing meaningful protection for the privacy and security of personal information. The Framework does not mandate legislation or any particular regulatory approach, but rather allows each Economy to come up with its own way of delivering the expected level of privacy protection. It is comprised of:

- A set of nine guiding APEC privacy principles
- Guidance on implementation to assist Economies in developing consistent domestic approaches to privacy protection
- A regional approach to promote accountable and responsible transfers of personal information between Economies.

[3] For more information, see Article 29 Data Protection Working Party, *Explanatory Document on the Processor Binding Corporate Rules* (19 April 2013) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf>.

The APEC CBPR System is the culmination of work by member Economies to develop a regional approach for personal information transfers. The system is intended to be applicable to any private sector organisation in the APEC region and comprises the following components:

- Internal rules adopted by organisations (and on behalf of their subsidiaries/affiliates) for a uniform approach to the access and use of personal information
- Privacy protection in line with the APEC privacy principles as well as internal processes similar to those required by BCR
- Establishment of Accountability Agent(s) in each participating Economy to certify the organisations' rules, monitor and enforce compliance, and resolve disputes between individuals and organisations
- Privacy Enforcement Authorities (PEAs) in each participating Economy enforcing the CBPR System and belonging to the Cross Border Privacy Enforcement Arrangement (CPEA).

2.4.2 OPERATION

In contrast to the self-contained operation of BCRs, there is a single CBPR System in which all companies participate.

Economies wishing to participate must receive approval from the Chair of the APEC Electronic Commerce Steering Group (ECSG). The participation criteria have been developed and agreed upon by all APEC Economies and include a number of requirements, such as having an acceptable Accountability Agent and a PEA that is a member of the CPEA. Applications to participate are assessed by the CBPR System's Joint Oversight Panel (JOP). The JOP advises the Chair of the ECSG as to how the requirements are met by the applicant Economy.

So far the United States and Mexico have been approved for participation in the CBPR System and Japan is currently seeking approval.

Once an Economy has been approved, companies in that Economy can self-assess their internal rules against the CBPR program requirements, which stipulate the base level of protection each company has to meet. After the self-assessment has been independently reviewed and certified by the Accountability Agent, the company is able to participate in the CBPR System, with the PEA acting as the enforcement backstop**.** In August 2013, IBM became the first company to be certified under the CBPR System.

It should be noted that the CBPR System is not legally binding on participating APEC Economies. The system is ultimately based on domestic legal components and is therefore subject to the laws of each Economy. Where domestic law conflicts with the CBPR program requirements, this could preclude the Economy from participation in the CBPR System.

At the same time, where the originating Economy has stronger privacy laws than the principles contained in the APEC Privacy Framework, the CBPR System allows the additional protections to be maintained following transfer.

2.4.2.1 TYPES OF TRANSFER

The APEC Privacy Framework distinguishes between data controllers and data processors in a way similar to the EU Data Protection Directive. An intake document with CBPR assessment criteria for controllers has been developed. Work is continuing on the assessment criteria for processors in recognition of their different responsibilities, in particular:[4]

- The willingness and capacity to help controllers honour their privacy obligations
- The willingness and capacity to maintain a secure platform when processing information on the controller's behalf.

The CBPR system will allow CBPR-certified companies to engage in the following types of personal information transfers:[5]

- Same company, different Economy – This is conceptually similar to BCR, where the transfer takes place between members of the same corporate group. For example, Google (Australia) transferring information about its users to Google (Singapore).
- Different company, different Economy (controller to controller) – For example, hotels.com (New Zealand) arranging a travel itinerary and transferring personal information to Shangri-La (Japan) to finalise accommodation.
- Different company, different Economy (controller to processor) – For example, Microsoft (Canada) transferring information to Accenture (US) for a digital marketing campaign.

What is achieved by CBPR varies across the Economies. In some cases – such as Australia, New Zealand, Hong Kong and Canada – there are legal requirements when transferring personal information overseas. In the future, participation in the CBPR System will provide a low friction way in which companies can meet those requirements.

For all Economies, regardless of whether they have introduced domestic privacy law, participation in the CBPR System will be beneficial for companies seeking a competitive advantage by increasing trust and confidence that their cross-border transfers will be safe.

2.5 ENFORCEMENT

As EU and APEC policymakers have made clear, it is not enough that there are rules in place that indicate to companies what is expected of them. Companies must also be held to account to ensure that the personal information is handled in accordance with the rules.

Both BCR and CBPR place great importance on enforcement. They require participating companies to have a mechanism for dealing with complaints. Furthermore, both systems require independent assurance that a participating company is in fact handling personal information in accordance with the rules.

[4] Centre for Information Policy Leadership, *CBPRs for Processors* (26 May 2012) <http://mddb.apec.org/Documents/2012/ECSG/DPS2/12_ecsg_dps2_003.pdf>. A draft Intake Questionnaire for Data Processors is currently under consideration by the ECSG and its Data Privacy Subgroup.

[5] For illustrative purposes certain Economies and companies are used in the examples that are not yet approved participants in the CBPR System.

External enforcement comes into play where the complaint cannot be resolved internally, the recommendations of the independent accountability agent are not followed, and/or there is a more serious breach of the rules. BCR and CBPR achieve this in similar but divergent ways, owing to the operational differences between the two systems.

2.5.1 Enforcement of BCR

BCRs are legally enforceable by:

- Individual data subjects – The company must provide data subjects with rights to enforce the BCR (third-party beneficiary rights), either via a unilateral declaration or by appropriate contractual arrangements. The data subject can choose to take action:
    - In the jurisdiction of the member that is at the origin of the transfer
    - In the jurisdiction of the EU headquarters or the jurisdiction of the European member with delegated data protection responsibilities ('the delegated member').

  In addition, data subjects always have the right to lodge a complaint before the DPA or the courts and seek enforcement in that way.
- DPAs – DPAs have investigatory and legal enforcement powers to supervise data transfers to destinations outside of the EU. By gaining approval of its BCR and receiving authorisation for international transfers on that basis, the company binds itself to the DPAs of the jurisdictions in which it operates to respect the safeguards contained in the BCR.
- Courts – Courts can enforce the BCR with respect to their jurisdiction over contractual disputes.

Where the BCR is breached by a member outside of the EU, the EU headquarters or the delegated member must accept responsibility and take necessary action to remedy the breach, including payment of compensation where appropriate. In order to discharge liability, the burden of proof is on the EU headquarters or delegated member to show that the member in question is not responsible for the breach.

2.5.2 Enforcement of CBPR

In addition to national Privacy Enforcement Authorities (PEAs) and the courts, the CBPR System introduces two new elements in order to ensure an effective enforcement framework when personal information moves between CBPR-certified companies: the Cross Border Privacy Enforcement Arrangement (CPEA) and the use of Accountability Agents.

2.5.2.1 Cross-border Privacy Enforcement Arrangement

The CPEA is the culmination of an APEC Data Privacy Pathfinder project that sought to find a solution to the problem that the supervision and enforcement of international transfers were beyond the capability of any single PEA.

Commencing on 16 July 2010, the CPEA created a multilateral mechanism for PEAs to cooperate in cross-border privacy enforcement.[6] The goals of the arrangement are to:

- Facilitate information sharing among PEAs in APEC Economies
- Provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, including through referrals of matters and through parallel or joint investigations or enforcement actions
- Encourage information sharing and cooperation on privacy investigation and enforcement with PEAs outside APEC.

PEAs are defined by the CPEA as any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings. Privacy Law is defined as laws and regulations of an APEC Economy which, when enforced, has the effect of protecting personal information consistent with the APEC Privacy Framework.

In order to participate in the CBPR System, an APEC Economy must have a PEA that is a participant in the CPEA. This is important because it demonstrates that the Economy has a law in place that has the effect of implementing the APEC Privacy Framework.

Current CPEA participants include Privacy Commissioners' offices (eg, the New Zealand Office of the Privacy Commissioner), consumer protection authorities (eg, the US Federal Trade Commission) and other government bodies (eg, Japan's Ministry of Justice).

2.5.2.2 Accountability Agents

To facilitate interoperability between the Economies and support and complement the role of PEAs, the CBPR System requires that each Economy nominate at least one organisation to be an Accountability Agent. The role of the Accountability Agent is to:

- Review a company's application and certify that it meets CBPR intake criteria and hence its eligibility to participate in the CBPR System
- Monitor the company throughout the certification period and advise the company on compliance with the CBPR program requirements
- Receive and investigate complaints about the company, and resolve disputes between complainants and the company
- Enforce the CBPR program requirements against the company, either through contract or by law.

An Accountability Agent may be a public or private organisation.[7] A PEA can also function as the Accountability Agent.

[6] APEC Committee on Trade and Investment, 'APEC Cross-border Privacy Enforcement Arrangement (CPEA)' <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>.

2.5.2.3 ENFORCEMENT PROCESS

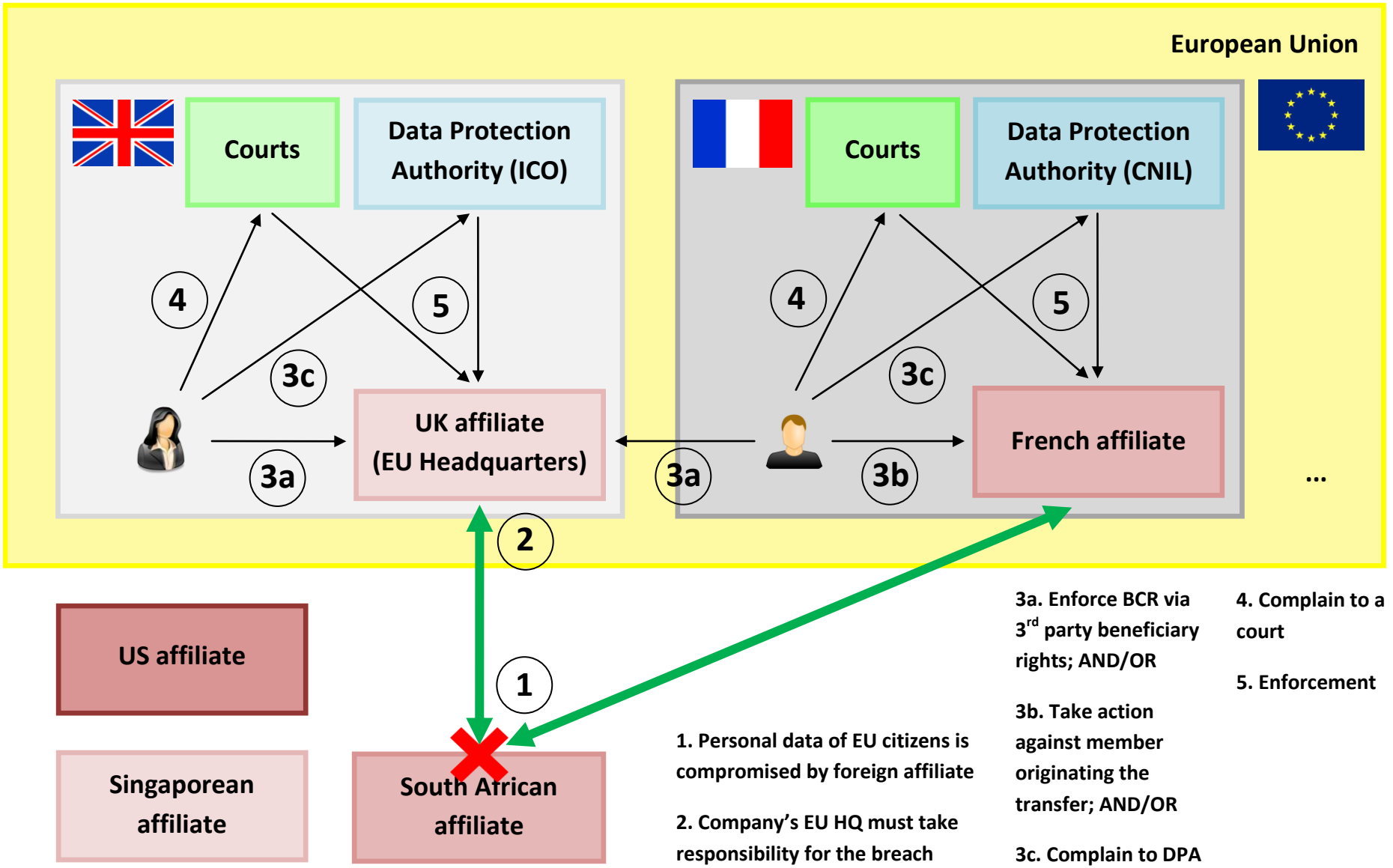
In the CBPR System, enforcement will ordinarily be carried out by the Accountability Agent, with the PEA acting as the backstop, in the following sequence:

- The Accountability Agent discovers that a CBPR-certified a company is not complying with the CBPR program requirements. This may occur through either:
    - Its regular monitoring processes
    - A direct complaint from an individual
- The Accountability Agent notifies the company, outlining the actions that must be taken to address the non-compliance within a reasonable period of time
- Failure to comply will lead to enforcement action by the Accountability Agent that is proportional to the harm or potential harm of the violation, including:
    - Removing the company from the CBPR System
    - Temporarily suspending the company's right to display the Accountability Agent's seal
    - Naming the company and publicising the non-compliance
    - Other penalties, including monetary penalties, compensation or other actions to make good the harm suffered by individuals
- Where the Accountability Agent is unable to resolve the problem and the failure is a violation of applicable privacy law, the Accountability Agent may refer the matter to the relevant PEA for review and possible law enforcement action
- The PEA may contact another CPEA participant for assistance or to make referrals regarding information privacy investigations and enforcement matters that involve the other's Economy.

The liability for violation of the CBPR program requirement(s) rests with the CBPR-certified company. Where a third party processor or controller is at fault, they may be obligated to provide compensation by the CBPR-certified company, such as through an indemnity clause.

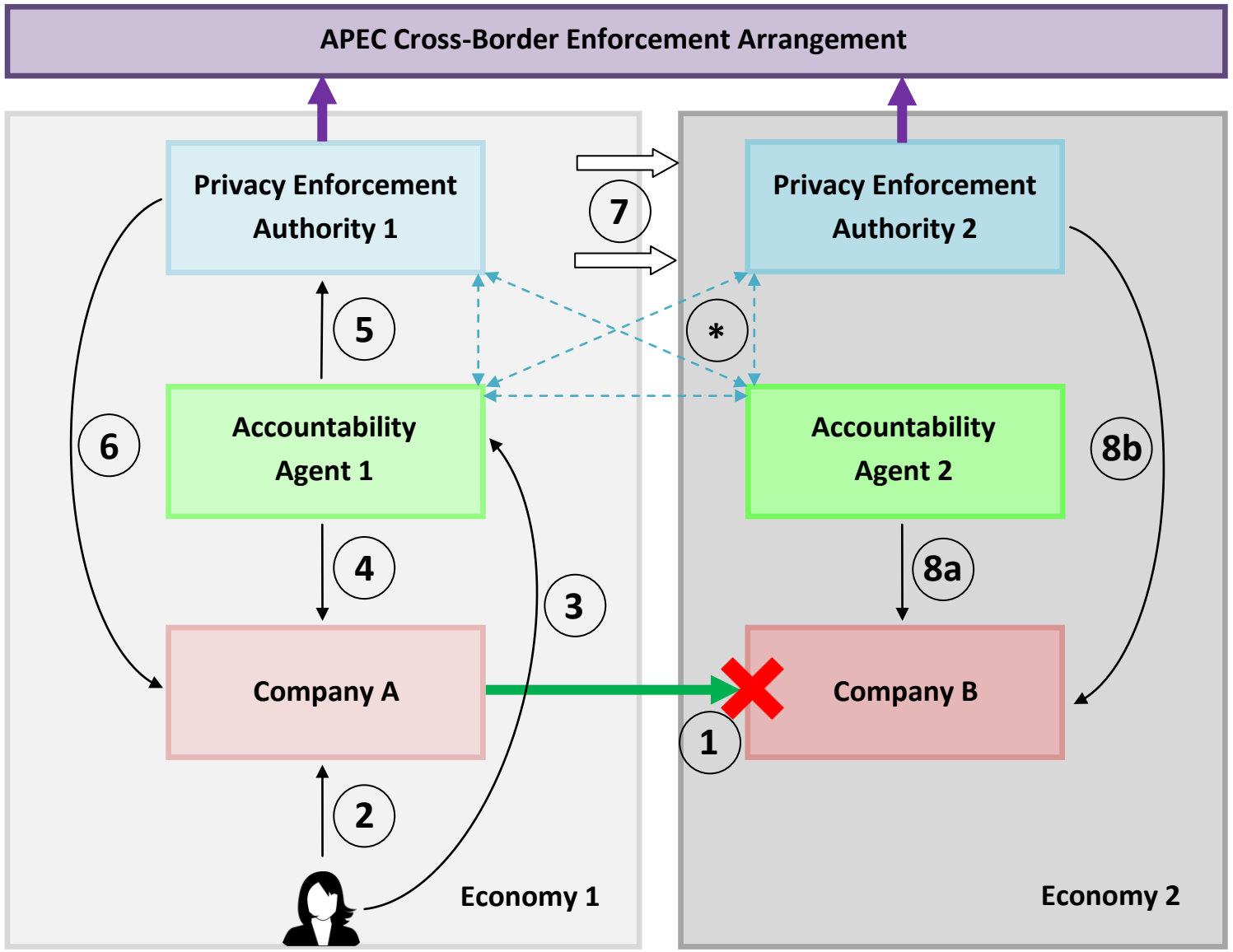
[7] For example, TRUSTe – an online privacy management services provider – has been selected to be the Accountability Agent for the United States. See TRUSTe, 'Press Release: TRUSTe Named First Accountability Agent for APEC Cross Border Privacy' (25 June 2013) <http://www.truste.com/about-TRUSTe/press-room/news_truste_named_first_agent_for_apec_cross_border_privacy>.

2.5.3 BCR ENFORCEMENT WORK-FLOW



2.5.4 CBPR ENFORCEMENT WORK-FLOW

The process described is illustrative only. The precise sequence will vary slightly depending on the Economy.



1. Personal information is transferred to Company B and a privacy breach occurs

2. Complain directly to Company A

3. If no resolution, complain to AA 1

4. Enforcement by AA 1

5. If no resolution, escalate to PEA 1

6. Enforcement by PEA 1

7. If no resolution in Economy 1, refer complaint to AA 2 and/or PEA 2 in Economy 2

8a. Enforcement by AA 2

8b. Enforcement by PEA 2

*** Cooperation where appropriate and possible**

3 HIGH-LEVEL COMPARISON

The following table contains the criteria for approval of a company's BCRs and the self-assessment criteria for a company's participation in the CBPR System.

WP #	Article 29 Working Party paper, with accompanying section number.
EU Directive #	Directive 95/46/EC (the Data Protection Directive), with accompanying article number.
PR #	APEC CBPR System program requirements, with accompanying section number.
AA #	Accountability Agent APEC recognition application, with accompanying paragraph number.
	There is no corresponding requirement in the other system and this is not of practical importance.
	The requirements are substantially similar.
	There is a notable but surmountable difference between the requirements.
	The requirements conflict or are otherwise incompatible.

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
1.	**BINDING NATURE – INTERNALLY**		
	1.1 Duty to respect the BCRs BCRs must contain a clear duty for all the members of the group and for the employees to respect the BCRs *WP 74 – 3.3.1*	**Ensure that employees are aware of the importance of, and obligations to the company with respect to, maintaining the security of personal information through regular training and oversight.**	BCRs must be made binding on the members of the corporate group and all employees. Most notably, any arrangement to

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	WP 108 – 5.3-5.9	Procedures may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other relevant practices. *PR – 29*	bind employees must be backed up by some form of sanction(s). While the CBPR program requirements do include internal policies and procedures for employees to safeguard the privacy and security of personal information, there is no explicit requirement for employees to be bound by them. **Possible bridging mechanism:** To the extent that it is necessary to enable data exchange in and out of the EU, this difference is surmountable. To achieve parity, the CBPR-certified company could include an internal binding mechanism.
	1.2 Application form to explain how rules are made binding on the members of the group and also the employees Rules binding companies/entities in the group may be one or more of the following: • Intra-group agreement • Unilateral undertakings • Internal regulatory measures • Policies of the group • Other means. Rules binding employees may be one or more of: • Individual and separate agreement/undertaking with sanctions • Clause in employment contract with sanctions • Internal policies with sanctions • Collective agreements with sanctions. *WP 74 – 3.3.1* *WP 108 – 5.3-5.9*		

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	BINDING NATURE – EXTERNALLY		
	1.3 Creation of third-party beneficiary rights for data subjects, including the possibility to lodge a complaint before the competent DPAs and before the courts. Data subjects must have rights to enforce the BCRs as third-party beneficiaries. These should cover judicial remedies for any breach of guaranteed rights and the right to receive compensation. *WP 74 – 3.3.2, 5.5.1 & 5.6* *WP 108 – 5.12-5.14, 5.16 & 5.20*	**Economies must have external enforcement mechanisms in place as a condition of participation in the CBPR System.** External enforcement takes place according to a hierarchy: • Individuals may complain to the Accountability Agent, who is responsible for investigating and resolving disputes between complainants and participating organisations • The Accountability Agent has authority to enforce the program requirements, either through contract or law • The Privacy Enforcement Authority steps in where there is a violation of local privacy law that upholds the APEC Privacy Framework and it is not resolved by the Accountability Agent.	The difference here is a matter of style rather than substance. In the EU, individuals can enforce the BCR directly via third-party beneficiary rights. Both the BCR and CBPR enable individuals to complain to the company directly and escalate to an external enforcement party if necessary. The CBPR System increases the capacity to hear and address complaints through the use of Accountability Agents in addition to the national PEA(s).

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	1.4 Company accepts liability for paying compensation and to remedy breaches of the BCR. *WP 74 – 5.5.1, 5.5.2 & 5.6* *WP 108 – 5.17*	**Applicant must describe the available remedial action relating to complaints.** The Accountability Agent must be satisfied by the proposed remedial mechanisms. CBPR-certified companies are bound to the rulings of the Accountability Agent and/or PEAs for paying compensation and otherwise remedying breaches. *PR – 43*	
	1.5 Application form to confirm that the company has sufficient assets. The application form must contain confirmation that the entity that has accepted the liability for the acts of other members linked by the BCRs outside of the EU has sufficient assets to pay compensation for damages resulting from the breach of the BCRs. *WP 74 – 5.5.2* *WP 108 – 5.17*		
	1.6 Burden of proof lies with the company not the individual. BCRs must state that the entity that has accepted liability will also have the burden of proof for demonstrating that the member of the group outside the EU is not liable for any violation of the rules which has resulted in the data subject claiming damages. *WP 74 – 5.5.2* *WP 108 – 5.19*	N/A	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	1.7 There is easy access to BCRs for data subjects and in particular easy access to the information about third-party beneficiary rights for the data subject that benefit from them. *WP 74 – 5.7*	N/A	Individuals will be able to access information about the CBPR System, the details of companies' certification and their rights on an APEC-hosted website. However, there is nothing in the CBPR program requirements that obliges the company to notify individuals of this information. **Possible bridging mechanism:** To the extent that it is necessary to enable data exchange in and out of the EU, this difference is surmountable. To achieve parity, the CBPR-certified company could provide information about their participation in the CBPR and the rights of individuals under the system, as well as linking to the relevant APEC website.
2.	**EFFECTIVENESS**		
	2.1 The existence of a suitable training programme. BCRs must state that appropriate training on the BCRs will be provided to personnel that:	**Procedures for training employees with respect to the Applicant's privacy policies and procedures, including how to respond to privacy-related complaints.**	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	• Have permanent or regular access to personal data • Are involved in the collection of personal data • Are involved in the development of tools used to process personal data. The training programme should be specified in the application. *WP 74 – 5.1* *WP 108 – 5.8 & 5.9*	*PR – 44*	
	2.2 The existence of a complaint handling process for the BCRs. Any data subject should be able to complain that any member of the group is not complying with the rules. The complaints must be dealt with by a clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions. The application form must explain how the data subject will be informed about the practical steps of the complaint system, for example: • Where to complain • In which form • Delays for the reply on the complaint • Consequences in cases of rejection of the complaint • Consequences in case the complaint is considered	**Procedures in place to receive, investigate and respond timely to privacy-related complaints.** Such procedures should include: • A description of how individuals may submit complaints to the company, and/or • A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information, and/or • A formal complaint-resolution process, and/or • Other relevant information. *PR – 41 & 42*	For both the BCR and CBPR, individuals can escalate their complaint to an external enforcement authority if the company does not provide a satisfactory response (see 1.3).

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	justified • Consequences if the data subject is not satisfied by the reply (eg, right to lodge a claim before a court/DPA). *WP 74 – 5.3* *WP 108 – 5.15, 5.18*		
	2.3 The existence of an audit programme covering the BCRs. The BCRs must provide for an audit programme: • That is conducted either: ○ On a regular basis (by either internal or external accredited auditors) or ○ On specific request from the privacy officer/function (or any other competent function in the organisation) • That covers all aspects of the BCRs, including methods of ensuring that corrective actions will take place • The result of which will be communicated to the privacy officer/function and to the parent company's board • The result of which is available for DPAs to access upon request. DPAs may also carry out data protection audits, subject to the investigatory powers they are given.	**Applicant must undertake risk assessments or certifications at appropriate intervals, and adjust its security safeguards to reflect the results of these assessments or certifications.** Privacy compliance audits may be conducted by the company. *PR – 34* The CBPR System obliges Accountability Agents to audit CBPR-certified companies throughout the certification period to ensure compliance with the program requirements. They must also verify whether recommendations made in the audits are implemented. *AA – Annex A, [6]-[8]*	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	WP 74 – 5.2 *WP 108 – 6*		
	2.4 The creation of a network of privacy officers or appropriate staff for handling complaints and overseeing and ensuring compliance with the rules. *WP 74 – 5.1 & 5.3*	**Applicant must designate an individual or individuals to be responsible for its overall compliance with the APEC Information Privacy Principles.** *PR – 40*	
3.	**COOPERATION DUTY**		
	3.1 A duty to cooperate with Data Protection Authorities. The BCRs should contain a clear duty for all members of the group to cooperate with, to accept to be audited by and to comply with the advice of DPAs on any issues related to the rules. *WP 74 – 5.4* *WP 108 – 5.21*	**Participation and cooperation with Accountability Agents and Privacy Enforcement Authorities is a fundamental requirement of companies seeking to participate in the CBPR System.**	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
4.	**DESCRIPTION OF PROCESSING AND DATA FLOWS**		
	4.1 A description of the transfers covered by the BCRs. The description should allow the DPAs to assess that the processing carried out in third countries is adequate, by describing: • The nature of the data transferred • The purposes of the transfer/processing • The data importers/exporters in the EU and outside of the EU. *WP 74 – 4.1* *WP 108 – 7*	**Description of personal information handling in the CBPR Intake Questionnaire.**[8] Description must include: • Type of personal information to be certified • APEC economies in which the personal information is collected • APEC economies to which personal information is transferred.	
	4.2 A statement of the geographical and material scope of the BCRs. The BCRs should indicate if they apply to: • All (or some) personal data transferred from the EU within the group, OR • All (or some) processing of personal data made within the group. The BCRs must also specify its material scope. Eg, stating that they apply to personal data related to employees, customers,		

[8] APEC Committee on Trade and Investment, *APEC Cross-Border Privacy Rules System Intake Questionnaire* <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.ashx>, pp 2-3.

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	suppliers and other third parties as part of the company's regular business activities. *WP 108 – 7.1.1 & 7.2*		
5.	**MECHANISMS FOR REPORTING AND RECORDING CHANGES**		
	5.1 A process for updating the BCRs. Where the BCRs are modified – eg, due to change in regulatory environment or company structure – the company must report changes to all group members and the DPAs. Updates to the BCRs or to the list of the members of the BCRs are possible without having to reapply for an authorisation, provided that: • An identified person keeps a fully updated list of the members of the group and keeps track of and records any updates to the rules and provides the necessary information to the data subjects or DPAs upon request • No transfer is made to a new member until the new member is effectively bound by the BCRs and can deliver compliance • Any substantial changes to the BCRs or to the list of members should be reported once a year to the DPAs granting the authorisations with a brief explanation of the reasons justifying the update. *WP 74 – 4.2*	**Updates to the company's privacy policy to be reviewed by the Accountability Agent.** Accountability Agents will require CBPR-certified companies to attest on an annual basis to the continuing adherence to the program requirements. Where there has been a material change to the company's privacy policy, an immediate review process will be carried out. The process includes: • An assessment of compliance, including verification of the company's updates • Report to the company outlining the Accountability Agent's findings, listing any corrections that the company needs to make • Verification that required changes have been completed by the company • Notice to the company that it is in compliance with the program requirements and has been re-certified. *AA – Annex A, [8]*	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	WP 108 – 9		
6.	**DATA PROTECTION SAFEGUARDS**		
	6.1 A description of the privacy principles including the rules on transfers or onward transfers out of the EU. *WP 74 – 3.1 & 3.2* *WP 108 – 8* The BCRs should explain how the following principles are observed in the company:	**Applicant must implement measures to ensure compliance with the APEC Information Privacy Principles.** *PR – 39* The Applicant must demonstrate compliance with the following principles:	
	i) Transparency, fairness *EU Directive – Arts 10 & 11*	**APEC Principle 2 – Notice** *PR – 1-4*	
	ii) Purpose limitation *EU Directive – Art 6(1)(a)-(c)*	**APEC Principle 3 – Collection limitation** *PR – 5-7* **APEC Principle 4 – Uses of personal information** *PR – 8-13*	
	iii) Data quality *EU Directive – Art 6(1)(d)*	**APEC Principle 6 – Integrity of personal information** *PR – 21-25*	Both sets of principles provide that personal data must be accurate, complete and kept up-to-date to the extent necessary. Importantly, the EU Directive also specifies that personal data should be kept for no longer than is necessary for the purposes for which the data was
	iv) Retention limitation		

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	EU Directive – Art 6(1)(e)		collected or for which they are further processed. It should be noted that some privacy laws in the APEC region have a similar requirement that would apply to transfers in the CBPR System. **Possible bridging mechanism:** To the extent that it is necessary to enable data exchange in and out of the EU, this difference is surmountable. To achieve parity, the CBPR-certified company could include a commitment to adopt a retention limitation policy.
	v) Security *EU Directive – Art 17*	**APEC Principle 7 – Security safeguards** *PR – 26-35*	The EU security principle requires contractual data protections when engaging subcontractors and processors. This is not mentioned in the APEC security principle, but a substantially similar obligation exists in the APEC accountability principle.
	vi) Right of access and rectification *EU Directive – Art 12*	**APEC Principle 8 – Access and correction** *PR – 36-38*	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	vii) Right to object to processing – general Individuals have the right to object (on compelling grounds) to the processing of their personal data by the data controller or by a third party to whom the data is disclosed. *EU Directive – Art 14(a)*	**APEC Principle 5 – Choice** Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. *PR – 14-20*	The APEC privacy principles do not have an explicit restriction on decisions made as a result of automatic processing. **Possible bridging mechanism:** To the extent that it is necessary to enable data exchange in and out of the EU, this difference is surmountable. To achieve parity, the CBPR-certified company could place safeguards on the automatic processing of personal information.
	viii) Right to object to processing – automatic processing Individuals have the right not to be subject to a decision which produces legal effects for him or her that is based solely on automated processing of data. *EU Directive – Art 15*		
	ix) Processing of special categories of data Subject to several exceptions, it is prohibited to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. *EU Directive – Art 8*	N/A	The APEC privacy principles do not have a provision addressing the handling of more sensitive categories information. However, some privacy laws in the APEC region do require additional protection for sensitive information as defined. CBPR ensures that those additional protections are respected. **Possible bridging mechanism:** To the extent that it is necessary to enable data exchange in and out of

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
			the EU, this difference is surmountable. To achieve parity, the CBPR-certified company can include appropriate extra protections on the handling of sensitive personal information.
	x) Restrictions on transfers and onward transfers to processors and controllers *outside of the EU*. Subject to the exceptions below, transfers to a third country for processing may take place only if the country in question ensures an adequate level of privacy protection. *EU Directive – Art 25* Exceptions: • Data subject has given his or her consent unambiguously, OR • The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request, OR • The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and third party, OR • The transfer is necessary or legally required on	**APEC Principle 9 – Accountability** There must be mechanisms in place to ensure that obligations to individuals are met when their personal information is processed by third parties (*whether domestic or international*) on the Applicant's behalf. Examples include: • Internal guidelines or policies • Contracts • Compliance with applicable industry or sector laws and regulations • Compliance with self-regulatory applicant code and/or rules • Other relevant practices. The mechanisms should generally require that the third party: • Abide by the Applicant's APEC-compliant privacy policies and practices as stated in the Privacy Statement, AND/OR • Implement privacy practices that are substantially	The EU and APEC allow for different ways of safeguarding personal information when it is transferred to a third party/jurisdiction, some of which overlap. The overarching idea is that an individual's personal information must continue to receive the same original protection regardless of where and to whom it is transferred.

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	important public interest grounds, OR • The transfer is necessary in order to protect the vital interests of the data subject. *EU Directive – Art 26(1)* • The Member State authorises the transfer where the company adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms, such as: o Use of contractual clauses, OR o Via the US-EU Safe Harbour Framework to a participating US organisation, OR o Via the BCRs to another intra-group entity. *EU Directive – Art 26(2)* • Use of standard contractual clauses approved by the European Commission. *EU Directive – Art 26(2)*	similar to the Applicant's privacy policies or practices as stated in the Privacy Statement, AND/OR • Follow instructions provided by the Applicant relating to the manner in which the personal information must be handled, AND/OR • Impose restrictions on subcontracting unless with the Applicant's consent, AND/OR • Participate in the CBPR System and have their CBPRs certified by an APEC Accountability Agent in their jurisdiction, AND/OR • Notify the Applicant in the case of a breach of personal information, AND/OR • Other relevant practices. *PR – 46 & 47*	
	N/A	**Third-party processors and service providers' compliance with the above mechanism(s) are confirmed by:** • **Self-assessments provided to the Applicant** • **Regular spot checking and/or monitoring by the Applicant.** *PR – 48 & 49*	

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	6.2 Application form should contain the list of entities bound by the BCRs *WP 108 – 7.1.3*	**Description of personal information handling in the CBPR Intake Questionnaire.** Description must include: • Name of organisation seeking certification, as well as subsidiaries and/or affiliates.	
	6.3 The need to be transparent where national legislation prevents the group from complying with the BCRs. Where a member of the group has reasons to believe that the applicable domestic law prevents the company from fulfilling its obligations under the BCRs and has substantial effect on the guarantees provided, the member will promptly inform: • The EU headquarters of the company, or • The EU member with delegated data protection responsibilities, or • The other relevant privacy officer/function. Where there is conflict between domestic law and the commitments in the BCR, one of the above parties will make a responsible decision on what action to take and will consult the competent DPAs in case of doubt. *WP 74 – 3.3.3*	N/A	BCR criterion 6.3 contemplates a scenario in which the BCR may conflict with the domestic law of a Member State and sets out possible action points. Such a situation would not arise with the CBPR. Where an Economy's domestic laws and regulations preclude or restrict that Economy's ability to participate in the CBPR System, it is a matter for the Economy to consider whether and how to modify the applicable domestic laws to facilitate participation before it can be accepted for participation.[9]

[9] APEC Committee on Trade and Investment, *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines* (2011) <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx>, p 11.

	Criteria for approval of BCRs	Criteria for participation in CBPR	Comments
	6.4 Although not required, it is useful to specify the relationship between the BCRs and the applicable domestic law. For example, the BCRs could state that, where the local legislation requires a higher level of protection for personal data, it will take precedence over the BCRs.	**The CBPR System does not displace or change an Economy's domestic laws and regulations.** Where there are no applicable domestic privacy protection requirements in an Economy, the CBPR System is intended to provide a minimum level of protection. Where domestic legal requirements exceed what is expected in the CBPR System, the full extent of such domestic law and regulation will continue to apply.	

4 DISCUSSION

4.1 THE CASE FOR A GLOBAL FRAMEWORK

Any consideration of global frameworks for the transfer of personal information across borders must take into account the tension that is building between the proliferation of privacy laws on the one hand and the rise of the global digital economy on the other.

Countries around the world are adopting privacy laws at an accelerating rate. Of the 99 countries that have adopted a comprehensive national data privacy law by June 2013, 8 did so in the 1970s, 13 in the 1980s, 21 in the 1990s, 35 in the 2000s and 22 in the first three years of the 2010s.[10] In the past three years, the APEC Economies of Singapore, Chinese Taipei, the Philippines and Malaysia have introduced comprehensive laws, although implementation in some cases has been slow.

At the same time, the flow of data has grown at a torrential rate. In 1992, global Internet traffic amounted to 100 gigabytes per day. This increased to 100 gigabytes per second in 2002 and 12,000 gigabytes per second in 2012.[11] With the advent of Web 2.0 in the 2000s and now the enormous uptake of mobile technology, the world has become a hyper-connected digital community. Today, the most successful and influential companies and economies are those that harness the power of data, and in particular, personal information.

These trends have no regard for national boundaries and national laws. However, individuals need protection more than ever as the collection, use and transfer of data expand in size and scope. If personal data is the new oil, then trust is the new currency.[12] As is the case with any currency, it is of most value when it is not debased. The goal should be widespread recognition and acceptance by individuals that companies will keep their information safe and that there are ways they can obtain effective remedy if something goes wrong.

A truly global framework for the safe and efficient transfer of personal information presents enormous benefits:

- For individuals:
    - Protection that travels with the data, so that data subjects covered by the framework is never without recourse to a remedy
    - Greater range of safe, innovative products and services that rely on far-ranging and unimpeded transfers of information

[10] Greenleaf, Graham, 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories', submitted to the *Journal of Law & Information Science* (16 June 2013) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877>; accompanied by the 'Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875>.

[11] Cisco, *The Zettabyte Era – Trends and Analysis* (29 May 2013) <http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.pdf>.

[12] World Economic Forum, *Rethinking Personal Data: Strengthening Trust* (May 2012) <http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf>.

- For companies:
    - Greater predictability and certainty in what rules to follow
    - Focus on effective data protection rather than inconsistent laws and compliance processes that can inhibit rather than facilitate it
    - Reduce cost by minimising patchwork solutions
    - More efficient transfer and processing of personal information
    - More open data transfers facilitate new business ideas and opportunities
    - Increase trust and build reputation
- For regulators:
    - Encourage compliance and shape norms in a collective and cohesive way
    - Increased onus on companies to be accountable and to meet the costs of compliance reduces the burden on regulators
    - Greater scope for international cooperation on specific cases as well as policy development.

BCR and CBPR are promising starts in achieving safe and efficient cross-border transfers at the regional level. IIS considers that the two systems will be important building blocks in establishing a truly global framework.

4.2 Assessment of BCR and CBPR

The comparison of BCR and CBPR yields no insurmountable conflict or incompatibility in terms of their participation criteria. There are however some noteworthy operational differences between BCR and CBPR, and they also provide different insights into a future global framework.

It should be noted that the BCR has been in place for several years, while CBPR is currently being rolled out. The purpose of the following analysis is to consider how they compare on the assumption that they are fully functioning as intended.

4.2.1 Scope of international transfers

A major difference between the two systems is their scope of operation.

BCR broke new ground by allowing companies to engage in low friction transfers between corporate members of the same group around the world, provided that they are subject to the same internal rules and the external supervision of a relevant EU DPA. However, international transfers outside the corporate group still require, for the most part, contractual provisions under Article 26(2) of the Data Protection Directive. As noted above, inter-group transfers can take place inside the EU without the need for BCR.

CBPR takes the next logical step by allowing for international inter-group transfers. That is, in addition to intra-group transfers, one CBPR-certified company in an Economy can transfer personal

information to another CBPR-certified company in a different Economy. This is made possible by the deliberate design of the CBPR System:

- The Cross-Border Enforcement Arrangement facilitates cooperation between PEAs in different Economies
- Economies seeking to participate must demonstrate that they have at least one PEA that is a member of the CPEA and that is capable of enforcing domestic law(s) with the effect of implementing the APEC Privacy Framework
- A mandate for Accountability Agents and PEAs from different Economies to work together.

The limitation of CBPR is that low friction transfers can only take place between APEC Economies that are participating in the CBPR System. Nevertheless, this provides a huge opportunity given that APEC Economies alone account for nearly half of all global trade and much of the recent economic growth.[13] As with the EU, transfers to third parties in other foreign destinations must take place using higher friction solutions such as suitable contractual arrangements.

The scope of operation of BCR and CBPR are circumscribed by corporate structure and geography, respectively. BCR's operational framework depends upon its EU-centric enforcement mechanism, in particular the requirement for a designated corporate headquarters located in the EU. On the other hand, the structure of the CBPR is more scalable. There is in principle no impediment to expanding the model beyond the APEC region in the future.

4.2.2 Content of privacy principles

A side by side comparison of the privacy principles underlying the BCR and CBPR reveals significant points of accordance as well as several noteworthy differences. Both the EU Data Protection Directive and the APEC Privacy Framework have principles addressing:

- Notice and transparency
- Purpose limitation regarding collection and use of personal information
- Data quality
- Data security
- Rights of access and correction
- Right to exercise choice over (and object to) how personal data is handled.

The Data Protection Directive contains additional principles relating to:

- Retention limitation
- Right to object to automatic processing of personal data

[13] Asia-Pacific Economic Cooperation, 'What is Asia-Pacific Economic Cooperation?' (2013) <http://www.apec.org/about-us/about-apec.aspx>.

- Restriction on the processing of sensitive personal data, eg, health information; racial or ethnic origin; political, religious or philosophical beliefs.

These legal differences are reflective of regional differences. The EU has the geopolitical cohesion required to adopt strong principles which reflect its approach to privacy as a fundamental human right. On the other hand, APEC is comprised of 21 Member Economies with diverse cultural values and political systems. While individual Economies such as Canada and New Zealand have privacy legislation that is close to the Data Protection Directive,[14] the APEC Privacy Framework was drafted at a more principled level in order to accommodate all 21 Economies.

4.2.2.1 STATUS OF DOMESTIC LAWS

In giving effect to the Data Protection Directive, the domestic laws of EU Member States feature some variations in terms of data protection. Indeed, achieving much greater harmony is one of the main objectives of the proposed EU Regulation now under consideration. The variation between domestic laws is addressed by BCR, which provides for the use of contracts to bridge the disparities between Member States.

There is a much greater variation between levels of protection provided by domestic law across the different APEC economies. Hence one of the challenges is to ensure that protections that are perceived to be 'higher' than the APEC Privacy Principles are not diminished should personal information protected at that level move to economies where the level of protection is perceived to be 'lower'. For example, Australia's Privacy Act has a specific definition of 'sensitive information' and requires additional protections when handling such information.

Currently, CBPR allows for several ways in which the higher protection may be enforced:

- Where the originating jurisdiction has domestic law that makes the sending company accountable to the individual for breaches caused by the receiving party – eg, section 16C of Australia's Privacy Act
- Where the recipient jurisdiction has broad-based consumer protection law that prohibits unfair or deceptive conduct, eg, section 5 of the United States Federal Trade Commission Act
- Where the sending company, regardless of domestic laws, contractually binds the receiving party to respect the higher level of protection.

The issue is that the current solutions are not applicable in all cases, and may not always minimise friction in cross-border transfers. Further clarification of how the CBPR system solves the challenge of ensuring higher domestic protection on personal information that is transferred to another jurisdiction may be required in the future.

4.2.3 IMPLEMENTATION OF RULES

Establishing rules for the safe transfer of personal information is an important step in any international framework. Just as important is the implementation of those rules. Both EU and APEC policymakers have been concerned to ensure effective implementation.

[14] Indeed, the Privacy Acts of both Canada and New Zealand have been deemed by the EU as ensuring an adequate level of protection.

4.2.3.1 BCR – FROM THEORY TO PRACTICE

BCR broke new ground by not only being the first cross-border system of its kind, but also in specifying in its approval criteria the practical steps necessary to carry out the rules.

In relation to the BCR's internal binding nature, the applicant company must oblige its group members and all employees to respect the rules. This duty is more than symbolic – the applicant company is required to take steps to make it binding, including:

- For group members:
    - Intra-group agreement
    - Unilateral undertakings
    - Internal regulatory measures
- For employees:
    - Clause in employment contract with sanctions
    - Internal policies with sanctions
    - Collective agreements with sanctions.

To establish the BCR's external binding nature, the applicant company must create third-party beneficiary rights for data subjects so that they can enforce the rules by complaining to a relevant DPA or before the courts.

To enhance the effectiveness of the BCR, the applicant company is required to implement:

- A suitable training program for employees that handle or make decisions about personal data
- A clear complaint handling process
- An audit programme that covers all aspects of the BCR
- A network of privacy officers or appropriate staff to handle complaints and ensure compliance with the rules.

These requirements are essential for bringing the rules for safe transfer of personal information from the realm of theory into actual effective practice. To highlight their importance, it can be seen from the comparison table that the CBPR Program Requirements contain very similar conditions.

4.2.3.2 CBPR – THE PREVENTING HARM PRINCIPLE

CBPR features many of the above implementation mechanisms. Rather than repeating them, it is worthwhile to consider some distinguishing aspects of the CBPR System.

The starting point is the APEC Privacy Framework's first principle: preventing harm. The principle recognises that a primary objective of the Privacy Framework is to prevent misuse of personal information and consequent harm to individuals. The principle also holds that remedial measures

should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

The Preventing Harm Principle is a pragmatic guideline that recognises the reality of enforcement – regulators have finite resources and so their efforts should be focused on where the harm is greatest.

4.2.3.3 CBPR – APEC ACCOUNTABILITY AGENTS

In the CBPR System, implementation of the rules is significantly boosted by the introduction of Accountability Agents. These bodies play a crucial role not only in assessing companies for participation, but also keeping them accountable through regular monitoring and acting as the first line of enforcement. Accountability Agents enhance implementation by:

- Providing individuals with another avenue (in addition to national regulators) to obtain independent third-party resolution of a problem or complaint
- Strengthening overall privacy protection – The protection of privacy is only as strong as the extent to which PEAs are resourced to do their job. By dealing with the first level of compliance and privacy complaints, Accountability Agents free up the PEA to deal with companies that are not part of the CBPR System.

It is envisaged that Accountability Agents will operate on a similar basis to auditors in the financial industry, where they are paid by the audit subject to conduct audits or other compliance checking processes with resources well beyond anything normally available to regulators. This is a proven model that will ensure the long-term sustainability of the CBPR System. There are strict rules regarding the independence and capabilities of eligible Accountability Agents and they are required to safeguard against potential and actual conflicts of interest.

4.2.4 ENFORCEMENT

4.2.4.1 OPERATION OF THE REGIMES

Aside from the use of Accountability Agents, the enforcement regime differs somewhat between BCR and CBPR due to their difference in scope.

BCR involves a company nominating a European entity (normally its EU headquarters or a member with delegated responsibilities) to be the focus of enforcement actions where a breach occurs in a non-EU jurisdiction. Cooperation beyond Europe is achieved by establishing intra-group obligations. This makes enforcement easier for individuals because rather than pursuing the member overseas, in a jurisdiction that may lack data protection law, European data subjects have a cause of action against a European entity.

On the other hand, CBPR contemplates transfers of personal information that are not intra-group in nature but still ensures a single point of contact for complaints at the first level for individuals. Transfers may involve multiple sending and receiving companies, taking place in multiple participating APEC Economies. Cross-border enforcement is therefore essential, which is why PEA participation in the CPEA is a prerequisite for an Economy to participate in the CBPR System.

A major advantage of this arrangement for companies is that in the CBPR System, companies operating in a participating Economy have the certainty of dealing with the local regulator(s). In the

BCR system, some companies have struggled with the idea that their non-EU members may be subject to an EU regulator, particularly if their centre of business is outside the EU.[15]

It is important to note that despite this outward difference, the underlying principle is the same for both BCR and CBPR: the sending company should be accountable for the information that it transfers outside of the EU or APEC Economy and the individual complainant should be able to gain accessible redress for violation of the relevant privacy requirements. BCR achieves this by specifying one responsible EU entity. The CBPR System does so by fostering cooperation between Accountability Agents and PEAs in the APEC Economies where the transfer takes place.

4.2.4.2 The power of individuals

Another point of difference is that BCR emphasises the ability of data subjects to legally enforce the rules, by requiring that they receive third-party beneficiary rights. On the other hand, the CBPR System contemplates that the Accountability Agent will take action to ensure that companies comply with its program requirements and address complaints.

Again, this outward difference masks substantial similarities. In both systems, individuals can bring complaints that become the catalyst for external enforcement action:

- In the EU, individuals can lodge a complaint with the relevant DPA(s) and/or courts
- In the APEC Economy, individuals can bring their complaint to the Accountability Agent and/or the PEA.

4.2.4.3 Coming together

In any further effort to increase cooperation between economies and regions, cooperation between APEC and EU enforcement bodies will be vital. The CPEA was developed with this in mind, one of its goals being to encourage information sharing and cooperation on privacy investigation and enforcement with authorities outside APEC.

While no formal arrangements have been announced, government authorities and regulators around the world have increasingly banded together to put pressure on companies over privacy issues, signifying a trend towards closer collaboration.

4.3 Facilitation of transfers between companies in the EU and APEC

Both the EU Data Protection Directive and the APEC Privacy Framework recognise that safe transfers of personal information beyond their direct reach must be possible. As mentioned earlier, the main means by which this is achieved in the EU is either at the jurisdictional level through findings of 'adequacy' or at the company level by model clauses, while in the APEC region they are recognised in questions 46 and 47 of the CBPR program requirements.

However, there is widespread agreement that these base mechanisms can be extremely time-consuming and costly. This has led to the work being initiated between officials of the EU Article 29 Working Party and APEC officials, with the hope that pathways can be developed that involve little or no friction.

[15] Allen & Overy, *Binding Corporate Rules* (February 2013) <http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf>, p 9.

4.3.1 LOW FRICTION LEGAL PATHWAYS BETWEEN THE EU AND APEC ECONOMIES

This section considers possible ways for interoperability between APEC and EU based on current understanding of how BCR and CBPR operate.

4.3.1.1 TRANSFER OF PERSONAL INFORMATION FROM AN EU COMPANY TO A CBPR-CERTIFIED COMPANY

Article 26 of the Data Protection Directive contains the exceptions to adequacy for personal data transfers from the EU to third party countries. Article 26(2) provides that a Member State may authorise the transfer where the company adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms. It is the means by which BCRs are approved for use in international data transfers.

However, the provision is open-ended – it is up to a company to satisfy a Member State that the safeguards are adequate by some means, including but not limited to 'appropriate contractual clauses'.

The flexibility of this provision means that it is conceivable for a company based in the EU to apply for authorisation of (ongoing) personal data transfer to a CBPR-certified company. To do so it must demonstrate that:

- The policies and rules of the receiving company provides similar data protection safeguards to the EU requirements
- There is both internal and external binding-ness.

Based on the high-level comparison above, IIS considers that there is a reasonable case to argue that CBPR requirements are substantially similar in most respects to the safeguards required by BCR which have been approved for use. In the short term, the few differences – namely, binding employees, providing notice on CBPR participation, establishing safeguards for automatic processing, the data retention limitation and restrictions on processing of sensitive data – can be bridged by additional undertakings on the part of the CBPR-certified company, to the extent that is necessary to enable data transfers in and out of the EU. In the longer term, differences might even be reflected in the rules of the CBPR System itself.

The main challenge is to guarantee external binding-ness – that is, the European data subject must be able to seek and receive redress if something goes wrong when their personal information is sent to a CBPR-certified company. This could entail:

- The existence of something like third-party beneficiary rights that allow individuals to seek a remedy from the CBPR-certified company[16]
- A mechanism by which EU and APEC privacy regulators can cooperate and recognise/address complaints from the other jurisdiction.[17]

[16] This would be akin to third-party beneficiary rights that exist in the BCR and also in the Model Contractual Clauses introduced by the European Commission.

[17] As noted above at 2.5.2.1, one of the express goals of the APEC CPEA framework is to encourage efforts to share information and cooperate on privacy matters with Privacy Enforcement Authorities outside the APEC region.

4.3.1.2 TRANSFER OF PERSONAL INFORMATION FROM A CBPR-CERTIFIED COMPANY TO THE EU

Where a CBPR-certified company needs to send personal information to the EU in the course of doing business, such a transfer will have to meet the APEC Privacy Framework requirements (in addition to any domestic laws).

CBPR is currently limited to the transfer of personal information between CBPR-certified companies in participating APEC Economies. Therefore, low friction transfers outside of the APEC region are not possible at this point.

To transfer personal information to the EU, the CBPR-certified company will need to use one or more of the methods outlined in questions 46 and 47 of the CBPR program requirement, such as:

- Internal guidelines or policies
- Contracts
- Compliance with applicable industry or sector laws and regulations
- Compliance with a self-regulatory organisation code and/or rules.

5 CONCLUSION

Careful analysis shows broad similarity between BCR and CBPR in their participation criteria. There are some differences in how the two systems operate, but nevertheless they largely aim to achieve the same ends of facilitating safe and efficient cross-border transfers of personal information.

BCR is the first cross-border system of its kind and introduces key concepts such as:

- The centrality for data subjects' rights to be respected and enforced regardless of where their data is transferred
- The notion that corporate rules must be binding both internally (relating to compliance in practice) and externally (relating to legal enforceability)
- The designation of a single corporate member to take responsibility when something goes wrong.

The CBPR System also has notable features, including:

- A broader scope by allowing low friction transfers between different companies
- The emphasis on cross-border regulatory cooperation, including both formal arrangements and operational requirements
- The use of independent third-party Accountability Agents, which emulates the financial information governance framework.

Together, BCR and CBPR provide an important foundation for a truly global framework for the safe and efficient transfer of personal information across borders.