Asia-Pacific
Economic Cooperation

2014/SOM1/ECSG/013
Agenda Item: IV1

APEC/EU Referential for the Structure of the EU Binding Corporate Rules and APEC Cross Border Privacy Rules System - Draft Endorsement Request

Purpose: Consideration
Submitted by: DPS Chair

APEC
CHINA 2014

29th Electronic Commerce Steering Group Meeting
Ningbo, China
20 February 2014

APEC/EU Referential for the Structure of the EU Binding Corporate Rules and APEC Cross Border Privacy Rules System
DRAFT Endorsement Request
SOM1 2014, Ningbo, China

OVERVIEW

On February 20, 2014, the Electronic Commerce Steering Group endorsed the APEC/EU Referential for the structure of the EU Binding Corporate Rules and APEC Cross Border, (hereinafter "Common Referential") developed by the BCR/CBPR Working Team.

The purpose of this document is to:

- seek endorsement for the Common Referential;
- provide an overview of the Common Referential and of the efforts of the Working Team;
- Provide an overview of a proposed March 2104 press event in Washington DC to mark the completion of the Common Referential;
- Outline next steps for the Working Team.

BACKGROUND

In September 2012 the Chair of the ECSG sought and obtained the approval of the SOM for the establishment of a joint Working Team consisting of interested APEC Economies and representatives from interested data protection authorities in the European Union Article 29 Working Party and from the European Commission. Since its inception, the Working Team has been engaged in the discussions regarding similarities and differences between the APEC Cross Border Privacy Rules System and the EU system of Binding Corporate Rules System.

These discussions led to the development and completion, in January 2014, of a Common Referential for the Structure of the EU System of Binding Corporate Rules and APEC Cross Border Privacy Rules System.

EU Binding Corporate Rules are one of selected mechanisms established by the EU to permit data about individuals to be transferred outside EU Member States. Such transfers are only permitted if "adequate" protection is provided for the personal data. BCRs provide such assurances of "adequate" protection for transfers taking place within a corporate group. This is accomplished through the establishment of binding internal corporate rules respecting the protection of personal data which all designated members of a corporate group are required to follow.

The CBPR System is a mechanism that confirms a baseline level of privacy protections across the APEC region and that facilitates transfers of personal information across the region. The system is one by which the privacy policies and practices of companies operating in the APEC region are assessed and certified by a Third party and demonstrated as following a set of commonly-agreed upon rules, based on the APEC Privacy Framework. By applying this commonly agreed-upon baseline set of rules, the CBPR system bridges across domestic differences that may exist amongst domestic privacy approaches.

PURPOSE OF COMMON REFERENTIAL

The common referential document outlines compliance and certification requirements of both the CBPR and BCR Systems, identifying elements that are common to both, as well as additional requirements for each. Exceptions and explanations are also provided where appropriate.

The referential is intended to be a high level guide and a pragmatic checklist for companies that engage in cross border commercial transactions involving international transfers of personal information and that are considering application for BCR and CBPR approval and certification. It aims to facilitate the implementation by these companies of policies and practices that will comply with the BCR and CBPR requirements.

The document does not constitute a mutual recognition between the two systems, nor does it establish new requirements for certification. Having used this document as general guidance, companies will still be expected to follow procedural requirements specific to each system for certification.

Because it aims to assist companies that are seeking certification under the CBPR system, the common referential is primarily of benefit to companies located in Economies that are CBPR participants, and of interest to Economies that are currently or are contemplating participation in the CBPR System.

NEXT STEPS

Following the completion of the Common Referential, The BCR-CBPR Working Team will continue its efforts to facilitate and support interoperability between the APEC and EU privacy regimes.

Further discussions and initiatives will be pursued, in support of trade between the two regions and to help build consumer trust about personal information protection both within, as well as outside the APEC region. The Working Team is considering ways in which elements of this work can be expanded to include non-governmental entities, including business and civil society representatives.

Conditional upon SOM endorsement, a Press event with representatives from the Article 29 Working Party and from interested APEC Economies, including the United States, is being planned during the upcoming IAPP World Summit Conference in Washington DC, in March 2014 to mark the occasion of the completion of the BCR/CBPR Common Referential. During the event, brief statements will be given by Economies and EU representatives to acknowledge the Common Referential as a step in the right direction for APEC/EU interoperability and recognize the ongoing collaboration between APEC economies and the European Union's Article 29 Working Party, and express the support of the United States for this effort.

Event participants from individual APEC member economies and EU Member States would be speaking on their own behalf and would not be speaking on behalf of APEC.

Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents

OVERVIEW

Aim of the referential:

The goal of this referential is to serve as an informal pragmatic checklist for organizations applying for authorization of BCR and/or certification of CBPR. It thereby facilitates the design and adoption of personal data protection policies compliant with each of the systems.

This referential does not aim at achieving mutual recognition of both systems. However, it could serve as a basis for **double certification.** In any case, data protection policies of applicant international companies operating both in the EU and the APEC areas **have to be approved respectively** by the relevant bodies in the EU Member States and in the APEC Economies, in accordance with the applicable approval procedures.

Background:

Experts from the Article 29 Working Party of Data Protection Authorities in the EU (hereinafter the "WP29")[1] and Member Economies from the APEC Data Privacy Sub-Group developed a practical tool to map the respective requirements of the BCR and the CBPR (hereinafter "referential") [2].

This referential lists in a single document the main elements generally required by national Data Protection Authorities in the EU (hereinafter "DPAs") on the one hand, and by the relevant bodies in APEC Economies on the other hand, in privacy policies submitted for authorization as a BCR by the national DPAs in the EU in accordance with data protection laws applicable in EU Member States, and/or as a CBPR in accordance with rules applicable in APEC Economies.

This referential was endorsed by APEC Senior Officials at their meeting of February 27-28, 2014, and the Article 29 Working Party adopted an opinion/working document on it at its plenary meeting of February 26-27, 2014.

Structure of the referential:

The referential comprises, for each of the essential principles and requirements of the systems:

- A "**common block**" describing the main elements which are common or similar to BCR and CBPR;

[1] The WP29 was set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It is composed of a representative of the supervisory authority (ies) designated by each EU Member State, a representative of the European Data Protection Supervisor and a representative of the European Commission. It has advisory status and acts independently.

[2] In the future, industry and civil society may provide input to APEC and to the WP29 in accordance with the APEC stakeholder engagement mechanisms and WP29 consultation mechanisms respectively.

- "**Additional blocks**" presenting their main differences and the additional elements specific to BCR on one hand and to CBPR on the other hand.

While the common block expresses a degree of commonality between what is mandatory in both CBPR and BCR systems, it is neither sufficient *per se* to obtain certification of a CBPR by an APEC recognized Accountability Agent, nor authorization of a BCR by a national DPA in the EU. In addition, the elements contained in the BCR additional block **must also be taken into account** by an organization applying for approval of its BCR by DPAs, and those listed in the CBPR additional block **shall also be taken into account** by an organization applying for certification of its CBPR by an APEC Accountability Agent.

REFERENTIAL ON REQUIREMENTS FOR BINDING CORPORATE RULES SUBMITTED TO NATIONAL DATA PROTECTION AUTHORITIES IN THE EU AND CROSS BORDER PRIVACY RULES SUBMITTED TO APEC CBPR RECOGNIZED ACCOUNTABILITY AGENTS

SUMMARY

Introduction

This document (hereinafter "referential") identifies the requirements common or similar to both the Binding Corporate Rules (hereinafter "BCR") as usually authorized by national Data Protection Authorities in the European Union (hereinafter "EU") for transfers of personal data outside of the EU but within a corporate group, and the Asia-Pacific Economic Cooperation (hereinafter "APEC") Cross Border Privacy Rules system (hereinafter "CBPR").

This referential also identifies the additional elements required for BCR approval and CBPR certification as regards the authorization and compliance review process of both national Data Protection Authorities in the EU (hereinafter "DPAs") and APEC CBPR recognized Accountability Agents. It is without prejudice to the individual authorization of BCR by national DPAs in line with EU data protection law and the certification of CBPR by APEC CBPR recognized Accountability Agents (hereinafter "APEC Accountability Agents"). It is also without prejudice to enforcement by the relevant supervisory and/or enforcement authorities.

This referential is not necessarily a comprehensive analysis of all elements of BCR and CBPR, nor the only way to map these two systems and should not be taken as legal advice, nor as reflecting the official position of any organization that participated in its development.

Purpose and Structure

This referential aims to facilitate an organization's implementation of personal data protection and privacy rules with a view to facilitating compliance with requirements as regards BCR and CBPR. It intends to serve as a pragmatic checklist for organizations that wish to design and implement privacy policies with a view to simultaneous application for authorization of a BCR by national DPAs in the EU and CBPR certification by an APEC Accountability Agent.

This referential is intended to be a comparative tool for use by those organizations considering application for BCR approval by national DPAs in the EU and CBPR certification by an APEC Accountability Agent, i.e. double certification. It is a comparison of the BCR and CBPR requirements in a single document to facilitate an organizations' formulation of personal data protection and privacy rules in view of meeting both systems' requirements and application of these personal data protection and privacy rules to its entities, subsidiaries and affiliates (hereinafter "the Group"). Formal determination of compliance with either system may only be accomplished through the appropriate recognized processes applicable in each system in line with the requirements set up by the applicable framework.

This referential is structured as follows: for each requirement identified there is a block of common or similar elements that are required both for BCR and for CBPR. Additional blocks for each BCR requirement and CBPR requirement follow, listing elements that are different in the two systems. These additional blocks may also list exceptions and clarifications of the requirements in the two systems. While the common blocks express a degree of commonality between what is required in both CBPR and BCR systems, they are neither sufficient *per se* to obtain certification of a CBPR by an APEC Accountability Agent, nor authorization of a BCR by a national DPA in the EU. In addition, the elements contained in the BCR additional blocks must also be taken into account by an organization applying for approval of its BCR by national DPAs

in the EU, and those listed in the CBPR additional block shall also be taken into account by an organization applying for certification of its CBPR by an APEC Accountability Agent.

It is noted that significant differences may exist between the requirements generally imposed by national DPAs in the EU for BCR authorization, in particular those deriving from EU data protection laws, and the CBPR program requirements. There are also differences between the respective objectives, scopes and review processes of the BCR and CBPR systems. As a result of such differences, some BCR and CBPR requirements are not fully compatible. Therefore, in order to avoid any conflict with applicable laws, applicant organizations shall make the scope of their personal data protection and privacy rules very clear. In their application, they shall clearly distinguish in which cases they will apply EU data protection laws and/or APEC CBPR program requirements, since personal data must be processed in accordance with the respective requirements of EU data protection law and/or the laws of APEC Economies.

An organization's personal data protection and privacy rules should be tailor-made in order to reflect the structure of the Group to which they apply, the processing undertaken by the Group, and the policies and procedures that they have in place to protect personal data. Therefore, organizations should note that national DPAs in the EU and CBPR-recognized Accountability Agents in APEC will not accept a pure copy and paste of this framework.

Scope

CBPR certification is limited to those organizations certified within a CBPR-participating Economy. The scope of a particular organization's CBPR certification will be limited to those entities, subsidiaries and affiliates identified in its application for CBPR certification.

Any organization wishing to transfer personal data from EU Member States to recipients located in non-EU countries may lodge an application with a national DPA in the EU for the approval of its BCR. The scope of a particular organization's BCR will be limited to those entities, subsidiaries and affiliates identified in its application for BCR approval. Correct implementation of the BCR, once approved, provides adequate safeguards for data transfers from such identified EU entities to the likewise identified non-EU entities, subsidiaries and affiliates (as specified in the organization's application).

The personal data protection and privacy rules applicable to cross border transfers of personal data can, if approved in accordance with the respective procedures, be capable of becoming the organization's or Group's policy for all personal data processed by the organization or Group as defined pursuant to its BCR approval by national DPAs in the EU and CBPR certification by APEC Accountability Agents. Where personal data is processed[3] in the EU[4], the requirements of

[3] The concept of processing includes storage, as well as any operation or set of operations which is performed upon personal data such as collection, recording, organization, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (See article 2(b) of Directive 95/46/EC).

[4] EU Member States' national data protection laws apply to the processing of personal data (including storage) where (a) the processing is carried out in the context of the activities of an establishment of the controller **on the territory of the EU**; (c) the controller is **not established in the EU** and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated in the EU, unless such equipment is used only for purposes of transit through the territory of the EU; (b) the controller is not established in the EU, but in a place where an EU Member State's national law applies by virtue of international public law (See Article 4(1) of Directive 95/46/EC).

EU data protection law also apply. Where personal data is processed in an APEC Economy, the laws of the relevant jurisdiction will apply.

This referential is based on the following documents:

EU:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, hereinafter "**Directive 95/46**";

- National laws implementing Directive 95/46/EC;

- *Working document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* (WP74), adopted by the Article 29 Working Party on 3 June 2003, hereinafter "**WP74**";

- *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules* (WP108), adopted by the Article 29 Working Party on 3 June 2003, hereinafter "**WP108**"

- *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (WP133), adopted by the Article 29 Working Party on 10 January 2007, hereinafter "**WP133**";

- *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules* (WP153), adopted by the Article 29 Working Party on 24 June 2008, hereinafter "**WP153**";

- *Working document setting up a framework for the structure of Binding Corporate Rules* (WP154), adopted by the Article 29 Working Party on 24 June 2008, hereinafter "**WP154**";

- *Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* (WP155), the Article 29 Working Party on 24 June 2008, as last revised and adopted on 8 April 2009, hereinafter "**WP155**".

APEC:

- *APEC Privacy Framework*, hereinafter "**Privacy Framework**"

- *APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines*, hereinafter "**Policies, Rules and Guidelines**"

- *APEC Cooperation Arrangement for Cross-Border Privacy Enforcement*, hereinafter "**CPEA**"

- *Template Notice of Intent to Participate in the APEC Cross-Border Privacy Rules System*, hereinafter "**Template notice of intent**"

- *Accountability Agent APEC Recognition Application*, hereinafter "**Recognition application**"

- *APEC Cross-Border Privacy Rules System Intake Questionnaire*, hereinafter "**Intake questionnaire**"

- *APEC Cross-Border Privacy Rules System Program Requirements*, hereinafter "**Program requirements**"

Referential on Personal Data Protection and Privacy Requirements of BCR and CBPR

1. Objective of an Organization's Personal Data Protection and Privacy Rules

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules should:

- Provide adequate protection for the transfer and processing of personal data by the Group as required under the BCR approval and CBPR certification processes [5]; and
- Constitute an enforceable obligation on the organization to ensure compliance with the personal data protection and privacy rules [6] (see sections 3 and section 21 of the referential);
- Contain reference to the applicable laws on data protection [7].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall contain a clear duty for all members of the Group and employees to interpret and respect the organization's personal data protection and privacy rules according to applicable laws [8].	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. Where requirements of the CBPR System exceed the requirements of domestic law and regulation, an organization will need to voluntarily carry out such additional requirements in order to participate. Nonetheless, Privacy Enforcement Authorities in that Economy should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements [9] (*see also 26, Relationship between local laws and the Organization's Personal Data Protection and Privacy Rules).*

References

[5] EU: see WP74, point 3.1, pp.7-9; APEC: see Privacy Framework, part iii, Principle I, 14, p.11

[6] EU: see WP154, Introduction, p.3 and WP74 p. 10-14; APEC: see CBPR Policies, Rules and Guidelines, 8, p.4; CBPR Program Requirements 39, 40

[7] EU: see WP154, Introduction, p.3; APEC: see Recognition application, Annex A, 4, p.5

[8] EU: see WP74, point 3.3.1, pp. 10-11; WP153, point 1.1, p. 3

[9] APEC: see Policies, Rules and Guidelines, 44, p. 10

2. Scope of an Organization's Personal Data Protection and Privacy Rules

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules should include a description of its scope of application including:

- The geographical scope (see sections 4 and 15 of this referential) [10];
- The material scope (i.e. nature of data, customers/prospective customers, employees/prospective employees, suppliers…) [11];
- The list of the entities bound by the organization's personal data protection and privacy rules [12]; and
- The purposes of the transfer and/or processing [13].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
The processing of personal data that is publicly available is subject to the requirements of EU data protection law and is not exempted from the BCR. Organizations that choose to participate in the BCR System shall implement privacy policies and practices consistently with the BCR program requirements for all personal data that is transferred within the Group outside of the European Union. While not required for BCR approval, participating organizations may apply the same privacy policies and procedures to all personal data that are processed within the Group globally, provided that compliance with EU data protection law is ensured where personal data is processed in the EU.	N/A
Clarification of the Scope of BCR	**Clarification of the Scope of CBPR**
N/A	In some instances, the organization's personal data protection and privacy rules may not apply to publicly available information [14]. Organizations that choose to participate in the CBPR System should implement privacy policies and practices consistently with the CBPR program requirements for all personal information that they have collected or received that is subject to cross-border transfer to other participating APEC

	Economies. While not required as part of the CBPR System, participating organizations are encouraged to apply the same privacy policies and procedures to all personal information that they have collected or received even if it is not subject to cross border transfer or if it is subject to such transfer only outside of participating APEC Economies [15].

References

[10] EU: see WP153, point 4.2 and WP108, point 7.1 and 7.2, pp.7-8; APEC: see Intake questionnaire, v-vi, pp.2-3

[11] EU: see WP153, point 4.2 and WP108, point 7.1.1 and 7.2, pp.7-8; APEC: see Intake questionnaire, iv, p.2

[12] EU: see WP153 point 6.2; WP108, point 7.1.3, p.8; APEC: see Intake questionnaire, ii, p.2

[13] EU: see WP153 point 4.1; WP108, point 7.1.2, p.8; APEC: see CBPR Program Requirement 1(b) and 1(c)

[14] APEC: see APEC Privacy Framework, 11 p. 7

[15] APEC: see Policies, Rules and Guidelines, 8, p. 4

3. Enforceable Obligation within an Organization

Common Elements Required for both BCR Approval and CBPR Certification

All entities of the Group seeking either approval of a BCR by a national DPA in the EU or certification of a CBPR by an APEC Accountability Agent must be subject to an enforceable obligation to comply with the organization's personal data protection and privacy rules under applicable laws that can be enforced by the individual/data subject and the regulator as appropriate [16].

Additional Elements Required for BCR Approval: Bindingness within a Group (BCR)	**Additional Elements Required for CBPR Certification**
The organization's personal data protection and privacy rules must be made legally binding between the entities in the Group by one or more of the following instruments [17]: i) Measures or rules that are legally binding on all members of the Group; ii) Contracts between the members of the Group; iii) Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the Group [18]; iii) Incorporation of other regulatory measures, for example, obligations contained in statutory codes within a defined legal framework; iv) Incorporation of the organization's personal data protection and privacy rules within the general business principles of an organization backed by appropriate policies, audits and sanctions; v) Other means [19]. In addition, the organization's personal data protection and privacy rules shall also be made legally binding on the employees by one or more of the following instruments [20]: i) Individual and separate agreement/undertaking with sanctions;	N/A

ii) Clause in employment contract with sanctions; iii) Internal policies with sanctions; iv) Collective agreements with sanctions.	
Clarification of Bindingness of an Organization (BCR) N/A	**Clarification of Accountability of an Organization (CBPR)** The organization must maintain its accountability by demonstrating the enforceability of its personal data protection and privacy rules through one or more of the following instruments [21]: i) Internal guidelines or policies; ii) Contracts; iii) Compliance with applicable industry or sector laws and regulations; iv) Other means. In addition, the organization shall have procedures in place for training employees with respect to its personal data protection and privacy rules [22].

References

[16] EU: see WP153 point 1.1 and 1.2; WP74, point 3.3.1, pp.10-11; APEC: see Program requirements, Q39, p.24; Annexes A and B

[17] EU: see WP153, point 1.2.i, p.3; WP108, point 5.6, p.5

[18] It is noted that in some EU Member States simple unilateral declarations may not be considered as legally binding under civil and administrative laws. In such a case, only contracts are regarded as binding. An organization would, therefore, need to take local advice if it intends to rely on other legal means than contracts.

[19] EU: WP74, point 3.3.1, pp. 10-11; WP153, point 1.1, p. 3

[20] EU: see WP74, point 3.3.1, pp.10-11; WP 153, point 1.1, p.3 and point 1.2.ii, p.3

[21] APEC: see Program requirements, Q39, p.24; Q46, p.26; Annexes A and B

[22] APEC: see Program requirements, Q44, p.25-26

4. Remedies for Data Subjects and Third Party Beneficiary Rights

Common Elements Required for both BCR Approval and CBPR Certification

N/A

Elements Required for BCR Approval	Elements Required for CBPR Certification
An organization's personal data protection and privacy rules shall clearly grant rights to data subjects to enforce the organization's personal data protection and privacy rules as third-party beneficiaries. They must outline the clear, accessible and effective judicial remedies for any breach of the personal data protection and privacy rules and the right to receive compensation (see articles 22 and 23 of EU Directive 95/46) [23]. An organization's personal data protection and privacy rules shall also contain a statement that data subjects have a right to choose any of the following routes to lodge a claim: - The jurisdiction of the data exporter located in the EU, or - The jurisdiction of the EU headquarters/the EU Member with delegated responsibilities, or - Before the competent national DPAs in the EU. An organization's personal data protection and privacy rules shall also contain the assurance that all data subjects beneficiating from the third party beneficiary rights will also have easy access to this clause [24].	An organization's personal data protection and privacy rules shall contain a statement that data subjects may enforce them through: - The controller's complaint resolution process [25]; or - The APEC Accountability Agent's dispute resolution process [26]. Data subjects shall also be able to lodge a complaint against an APEC Accountability Agent directly to the Joint Oversight Panel [27]. An organization's personal data protection and privacy rules shall also contain a requirement that data subjects may lodge a complaint before APEC Accountability Agents [28]. Depending on CBPR participating Economies, data subjects may have a private right of action built in to their local data privacy laws, which may be used to enforce CBPR compliance.

References

[23] EU: see WP74, point 3.3.2, pp.11-13

[24] EU: see WP153, point 1.7, p.5

[25] APEC: see Intake questionnaire, Q41-43, pp.21-22

[26] APEC: see Recognition application, Annex A, 9-10, p.7

[27] APEC: see Policies, Rules and Guidelines, 35, p.9

[28] APEC: see Recognition application, Annex A, 9-10, p.7

5. Liability

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall provide, as a principle, that liability lies on one entity [29].

Additional Elements Required for BCR Approval	Additional Elements Required for CBPR Certification
An organization's personal data protection and privacy rules shall also contain a commitment that [30]: - Either EU headquarters or the EU Member with delegated responsibilities accept responsibility for and agree to take the necessary action to remedy the acts of other Members of the Group outside of the EU and to pay compensation for any damages resulting from the violation of an organization's personal data protection and privacy rules by the members of the Group. - The burden of proof stays with either the EU headquarters or the EU Member with delegated responsibilities to demonstrate that the member outside the EU is not liable for the violation resulting in the damages claimed by the data subject. If the EU headquarters or the EU Member with delegated responsibilities can prove that the member outside the EU is not liable for the violation, it may discharge itself from any responsibility. If this is not possible for some groups with particular corporate structures to impose to a specific entity to take all the responsibility for any breach of BCR out of the EU, national DPAs in the EU might accept other liability mechanisms on a case-by-case basis if sufficient comfort is provided that data subjects rights will be enforceable and they will not be disadvantaged in enforcing them [31].	An organization's personal data protection and privacy rules shall also contain a commitment that liability lies with the CBPR-certified entity. However, this does not displace any additional liability of subsidiaries/affiliates under the local laws in which a violation may have occurred.

References

[29] EU: see WP74, point 5.5.2, pp.18-19; APEC: see Intake questionnaire, ii, p.2

[30] EU: see WP74, point 5.5.2, pp.18-19

[31] Such possible liability schemes would be the joint liability mechanism between the data importers and the data exporters as seen in the EU Standard Contractual Clauses 2001/497/EC dated June 15, 2001 or to define an alternative the liability scheme based on due diligence obligations as prescribed in the EU Standard Contractual Clauses 2004/915/EC dated December 27, 2004. A last possibility, specifically dedicated to transfers made from controllers to processors is the application of the liability mechanism of the Standard Contractual Clauses 2002/16/EC dated December 27, 2001.

6. Enforceable Obligations regarding Transfers to Third Parties

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall contain an enforceable obligation that the organization transfers data only to third parties that apply protection to the processing of personal data, as well as an explanation of how the organization's personal data protection and privacy rules are made enforceable upon such recipients of data in the relevant jurisdiction [32].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall contain rules to restrict transfers and onward transfers outside of the Group and an obligation to ensure that [33]: - External processors located inside the EU or in a country recognized by the European Commission as ensuring an adequate level of protection shall be bound by a written agreement stipulating that the processor shall act only on instructions from the controller and shall be responsible for the implementation of the adequate security and confidentiality measures; - All transfers of data to external controllers located outside of the EU and not in a country recognized by the European Commission as ensuring an adequate level of protection must respect the European rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC: for instance making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC or by other appropriate contractual means in accordance with Articles 25 and 26 of the EU Directive); - All transfers of data to external processors located out of the EU must respect the rules relating to the processors (Articles 16-17 Directive	N/A

95/45/EC) in addition to the rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC).	
Clarification of Bindingness on Third Parties (BCR) N/A	**Clarification of Accountability in respect of transfers to Third Parties (CBPR)** An organization's personal data protection and privacy rules shall contain an explanation of how personal data are protected when using a processor, agent, contractor or other service provider. In particular a requirement that: - The controller must choose a processor, agent, contractor or other service provider providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures [34]; - The controller shall instruct the processor to ensure in particular that: i) The processor, agent, contractor or other service provider shall act only on instructions from the controller [35]; ii) The rules relating to the security and confidentiality to be incumbent on the processor, agent, contractor or other service provider [36]. An organization's personal data protection and privacy rules can be made binding by one or more of the following instruments [37]: i) Internal guidelines or policies; ii) Contracts; iii) Compliance with applicable industry or sector laws and regulations; iv) Other means.

References

[32] EU: see WP74, point 3.2, pp.9-10; APEC: see Program requirements, Q39, p.24; Q46, p.26; Annexes A and B; Intake questionnaire, Q47, p.22

[33] EU: see WP153, point 6.1 vi); WP154, point 12, p.7

[34] APEC: see Intake questionnaire, Q35, p.15

[35] APEC: see Intake questionnaire, Q47-48, pp.22-23

[36] APEC: see Intake questionnaire, Q35, pp.15-16

[37] APEC: see Program requirements, Q39, p.24; Q46, p.26; Annexes A and B

7. Relationships with Processors that are Members of the Group

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall contain an explanation of how personal data are protected when using a processor who is a member of the Group, in particular a requirement that [38]:

- The controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures [39];
- The controller shall instruct the processor to ensure in particular:
  - That the processor shall act only on instructions from the controller [40];
  - The rules relating to the security and confidentiality to be incumbent on the processor [41].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall provide a commitment that instructions shall be given by written contractual means in accordance with the applicable law [42].	When the controller intends to transfer personal data to processors, agents, contractors or other service providers, he/she should obtain the consent of the data subject or exercise due diligence, and take reasonable steps to ensure that the recipient person or organization will protect the data consistently with the organization's personal data protection and privacy rules [43]. In situations where due diligence and reasonable steps to ensure compliance with the organization's personal data protection and privacy rules is impractical or impossible, the controller shall provide an explanation and describe the other means used for ensuring that the data, nevertheless, is protected consistent with the APEC Privacy Principles. Instructions may be given by the controller through [44]: - Internal guidelines or policies; or - Contracts; or - Compliance with applicable industry or sector laws and regulations; or

	- Compliance with self-regulatory organization code and/or rules; or - Other means. Such agreements shall generally require that personal data processors, agents, contractors or other service providers [45] include appropriate protections from the following options: - Abide by the controller's APEC-compliant privacy policies and practices as stated in the controller's Privacy Statement; - Implement privacy practices that are substantially similar to the controller's policies or privacy practices as stated in the controller's Privacy Statement; - Follow instructions provided by the controller relating to the manner in which the controller's personal data must be handled; - Impose restrictions on subcontracting unless with the controller's consent; - Have their CBPRs certified by an APEC Accountability Agent in their jurisdiction; Processors, agents, contractors or other service providers shall notify the controller when they become aware of an occurrence of breach of the privacy or security of the personal data of the controller's personal data [46]. Processors, agents, contractors or other service providers shall take immediate steps to correct/address the security failure which caused the privacy or security breach [47]. Processors, agents, contractors or other service providers shall provide the controller with self-assessments to ensure compliance with the controller's instructions and/or agreements/contracts [48]. The controller shall carry out regular spot checking or monitoring of his/her personal data processors, agents, contractors or other

	service providers to ensure compliance with his/her instructions and/or agreements/contracts [49].

References

[38] EU: see Directive 95/46, art. 17.2; WP154, point 11, pp.6-7

[39] APEC: see Intake questionnaire, Q35, p.15

[40] APEC: see Intake questionnaire, Q47-48, pp.22-23

[41] APEC: see Intake questionnaire, Q35, pp.15-16

[42] EU: see Directive 95/46, art. 17.2; WP154, point 11, pp.6-7

[43] APEC: see Privacy Framework, part iii, Principle IX, 26, p.28

[44] APEC: see Intake questionnaire, Q46, p.22

[45] APEC: see Intake questionnaire, Q47, pp.22-23

[46] APEC: see Intake questionnaire, Q35-b), p.15

[47] APEC: see Intake questionnaire, Q35-c), p.16

[48] APEC: see Intake questionnaire, Q48, p.23

[49] APEC: see Intake questionnaire, Q49, p.23

8. Restrictions on Transfers and Onward Transfers to External Processors and Controllers (not Members of the Group)

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall contain the requirement that contractors which receive data and process them shall be required to protect personal data in accordance with the transferring organization's personal data protection and privacy rules [50].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also contain an explanation of the measures in place to restrict transfers and onward transfers outside of the group and an obligation to ensure that: - External processors located inside the EU or in a country recognized by the European Commission as ensuring an adequate level of protection shall be bound by a written agreement stipulating that the processor shall act only on instructions from the controller and shall be responsible for the implementation of the adequate security and confidentiality measures [51]; - All transfers of data to external controllers located outside of the EU or not in a country recognized by the European Commission as ensuring an adequate level of protection must respect the European rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC: for instance making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC or by other appropriate contractual means in accordance with Articles 25 and 26 of the EU Directive) [52]; - All transfers of data to external processors located out of the EU must respect the rules relating to the processors (Articles 16-17 Directive	An organization's personal data protection and privacy rules shall also contain an explanation of how personal data are protected when using a processor, agent, contractor or other service provider. In particular a requirement that: - The controller must choose a processor, agent, contractor or other service provider providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures [54]; - The controller shall instruct the processor, agent, contractor or other service provider to ensure in particular that: i) it shall act only on instructions from the controller [55]; ii) it observes the rules relating to the security and confidentiality to be incumbent on the processor, agent, contractor or other service provider [56]. Instructions may be given by the controller through [57]: - Internal guidelines or policies; or - Contracts; or - Compliance with applicable industry or sector laws and regulations; or

95/45/EC) in addition to the rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC) [53].	- Compliance with self-regulatory organization code and/or rules; or - Other means. Such agreements shall generally require that personal data processors, agents, contractors or other service providers include appropriate protections from the following options [58]: - Abide by the controller's APEC-compliant privacy policies and practices as stated in the controller's Privacy Statement; - Implement privacy practices that are substantially similar to the controller's policies or privacy practices as stated in the controller's Privacy Statement; - Follow instructions provided by the controller relating to the manner in which the controller's personal data must be handled; - Impose restrictions on subcontracting unless with the controller's consent; - Have their CBPRs certified by an APEC Accountability Agent in their jurisdiction; - Other means. Processors, agents, contractors or other service providers shall notify the controller when they become aware of an occurrence of breach of the privacy or security of the personal data of the controller's personal data [59]. Processors, agents, contractors or other service providers shall take immediate steps to correct/address the security failure which caused the privacy or security breach [60]. Processors, agents, contractors or other service providers shall provide the controller with self-assessments to ensure compliance with the controller's instructions and/or agreements/contracts [61]. The controller shall carry out regular spot

	checking or monitoring of his/her personal data processors, agents, contractors or other service providers to ensure compliance with his/her instructions and/or agreements/contracts [62].

References

[50] EU: see WP74, point 3.2, pp.9-10; APEC: see Intake questionnaire, Q47, p.22

[51] EU: see Directive 95/46, art. 17.2; WP154, point 12, p.7

[52] EU: see WP74, point 3.2, pp.9-10

[53] EU: see WP154, point 12, p.7

[54] APEC: see Intake questionnaire, Q35, p.15

[55] APEC: see Intake questionnaire, Q47-48, pp.22-23

[56] APEC: see Intake questionnaire, Q35, pp.15-16

[57] APEC: see Intake questionnaire, Q46, p.22

[58] APEC: see Intake questionnaire, Q47, pp.22-23

[59] APEC: see Intake questionnaire, Q35-b), p.15

[60] APEC: see Intake questionnaire, Q35-c), p.16

[61] APEC: see Intake questionnaire, Q48, p.23

[62] APEC: see Intake questionnaire, Q49, p.23

9. Definitions

Common Elements Required for both BCR Approval and CBPR Certification

An organization is expected to interpret the terms in its personal data protection and privacy rules according to applicable EU laws, in particular Directive 95/46/EC and Directive 2002/58/EC, applicable laws in CBPR-participating Economies and the APEC CBPR glossary [63].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall contain a commitment to interpret the terms according to applicable EU laws, in particular Directive 95/46/EC and Directive 2002/58/EC, and shall contain a description of the main terms and their definitions: personal data [64]; controller [65]; processor [66]; data subjects [67]; sensitive personal data [68]; processing [69]; third party [70]; and EU Data Protection Authorities [71].	N/A

References

[63] EU: see WP154, point 2, p.4; WP155 Q8, p.5; APEC: see CBPR Glossary

[64] EU: see Directive 95/46, art. 2-a

[65] EU: see Directive 95/46, art. 2-d

[66] EU: see Directive 95/46, art. 2-e

[67] EU: see Directive 95/46, art. 2-a

[68] EU: see Directive 95/46, art. 8

[69] EU: see Directive 95/46, art. 2-b

[70] EU: see Directive 95/46, art. 2-f

[71] EU: see Directive 95/46, art. 2-f

10. Collection, Processing and Use of Personal Information

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall provide that personal data shall only be collected and processed fairly and lawfully [72] for specified purposes and cannot be used in a way incompatible with those purposes as that term may be defined by applicable law [73].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also provide that personal data will only be transferred and processed for explicit and legitimate purposes [74].	N/A
Clarification of Processing of Personal Data (BCR)	**Clarification of Use of Personal Information (CBPR)**
N/A	Personal information can be used for other compatible or related purposes with the consent of the individual whose personal information is collected; when necessary to provide a service or product requested by the individual; or by the authority of law and other legal instruments, proclamations and pronouncements of legal effect [75].

References

[72] EU: see Directive 95/46, art. 6.1-a; WP108, point 8.2.1, p.8; WP153, point 6.1.i, p.10; WP154, point 5, p.4, point 6, p.5; APEC: see Privacy Framework, part iii, Principle III, 18, p.15; Program Requirements, Q7, p.7

[73] EU: see Directive 95/46, art. 6.1-b; WP108, point 8.2.2, p.8; WP153, point 6.1.ii, p.10; WP154, point 3, p.4; APEC: see Privacy Framework, part iii, Principles III & IV, 18 and 19, p.15-16, Program Requirements, Q6, and Q8, p 6 & 8

[74] EU: see Directive 95/46, art. 6.1-b; WP108, point 8.2.2, p.8; WP153, point 6.1.ii, p.10; WP154, point 3, p.4

[75] APEC: see Privacy Framework, part iii, Principle IV, 19, pp.16-17, Program Requirements, Q9 &13, pp.8-10

11. Data Quality and Proportionality / Integrity

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall contain a commitment that:

- Personal data shall be accurate, complete and where necessary, kept up-to-date. An organization's personal data protection and privacy rules shall also contain a commitment to communicate those corrections to all relevant parties where appropriate [76].
- Personal data shall be adequate and relevant in relation to the purposes for which they are transferred and/or further processed [77].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also contain an explicit requirement that personal data are not excessive in relation to the purposes for which they are transferred and further processed [78]. An organization's personal data protection and privacy rules shall also contain a requirement that personal data may not be processed for longer than necessary for the purposes for which they are obtained, or if necessary, further processed [79].	N/A

References

[76] EU: see Directive 95/46, art. 6.1-d; WP153 point 6.1.iii, p.10; WP108, point 8.2.3, p.8; APEC: see Privacy Framework, part iii, Principle VI, 21, p.20; Program Requirements 21; 22, p.15; Intake questionnaire Q22, Q23 and 24, p.13

[77] EU: see Directive 95/46, art. 6.1-c; WP153 point 6.1.iii, p.10; WP108, point 8.2.3, p.8; APEC: see Privacy Framework, part iii, Principle III, 18, p.15, Program Requirements, Q6, p.6

[78] EU: see Directive 95/46, art. 6.1-d; WP153 point 6.1.iii, p.10

[79] EU: see Directive 95/46, art. 6.1-e; WP153 point 6.1.iii, p.10; WP108, point 8.2.3, p.8

12. Grounds for Processing Personal Data

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall contain a commitment that:

- Personal data shall only be processed (including collected, used, transferred, disclosed or made available) when there is a valid ground for processing, such as where the individual/data subject has given his or her informed consent [80].
- Personal data shall be processed consistently with the applicable law [81].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
Where consent is the legal basis for processing, it shall be unambiguous, specific, freely given and informed [82]. Consent as a legal basis for processing cannot be displaced on grounds of obviousness, nor that the personal data is publicly available, nor that consent is technologically impracticable, nor that the personal data was received from a third party. Consent is only one of the possible legal basis for the processing of personal data. Personal data may also be processed based on the following grounds [83]: - The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or - The processing is necessary for compliance with an EU legal obligation to which the controller is subject; or - The processing is necessary in order to protect the vital interests of the data subject; or - The processing is necessary for the performance of a task carried out in the public interest or in the exercise of EU official authority vested in the controller or in a third party to whom the data are	N/A

disclosed; or - The processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.	
Clarification of Grounds for Processing (BCR) N/A	**Clarification of Grounds for Processing (CBPR)** Individuals shall be provided with choice in relation to collection, use, and disclosure of their personal information. However, this principle recognizes, through the introductory words "where appropriate" in the Privacy Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in "Qualifications to the Provision of Choice Mechanisms" [84]. Subject to the listed qualifications, individuals shall be given: - A clear and conspicuous mechanism to exercise choice in relation to the collection of their personal information. - A clear and conspicuous mechanism to exercise choice in relation to the use of their personal information - A clear and conspicuous mechanism to exercise choice in relation to the disclosure of their personal information - These mechanisms must be clearly worded, easily understandable, easily accessible and affordable. Applicable qualifications include:

	- Obviousness; - Collection of Publicly-Available Information; - Technological Impracticability; - Third-Party Receipt; - Disclosure to a government institution which has made a request for the information with lawful authority; - Disclosure to a third party pursuant to a lawful form of process; - For legitimate investigation purposes; - Action in the event of an emergency. Apart from consent, personal data may also be processed based on the following grounds [85]: - For compatible or related purposes as identified in the privacy statement and/or in the notice provided at the time of collection; - Necessary to provide a service or product requested by the individual; - Compelled by applicable laws.

References

[80] EU: see Directive 95/46, art. 7-a; WP154, point 5, p.4; APEC: see Privacy Framework, part iii, Principle III, 18, p.15

[81] EU: see WP153, point 6.4, p.11; WP155 Q10, p.6; APEC: see Program Requirements, Q7, p.7

[82] EU: see Directive 95/46, art. 7-a; WP154, point 5, p.4

[83] EU: see Directive 95/46, art. 7; WP154, point 5, p.4

[84] APEC: see Program Requirements Q14; 15; 16; 17; 18; 19, pp. 11-14

[85] APEC: see Program Requirements Q8; 9; 10; 11; 12; 13, pp. 8-10

13. Sensitive Data

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall identify the protections applicable to sensitive data [86].

Additional Elements Required for BCR Approval	Additional Elements Required for CBPR Certification
An organization's personal data protection and privacy rules shall also contain a commitment that processing of sensitive data (e.g., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, concerning sex life, or health data) is prohibited except if [87]: - The data subject has given his/her explicit consent to the processing of those sensitive data, except where the applicable laws prohibit it; or - The processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of EU employment law insofar as it is authorized by national law providing for adequate safeguards; or - The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or - The processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party	In determining the permitted uses of information, the nature of the information must be considered [89]. Security safeguards that are implemented shall be reasonable and proportional to the likelihood and severity of the harm threatened, the sensitivity of the data and the context in which it is held [90].

without the consent of the data subjects; or - The processing relates to sensitive data which are manifestly made public by the data subject; or - The processing of sensitive data is necessary for the establishment, exercise or defense of legal claims; or - The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. Sensitive data should be processed with enhanced security measures [88].	

References

[86] EU: see Directive 95/46, art. 8; WP154, point 6, p.5; APEC: see Privacy Framework, part iii, Principle VII, 22, p.21

[87] EU: see Directive 95/46, art. 8; WP154, point 6, p.5

[88] EU: see Directive 95/46, art. 17.1; WP154, point 10, p.7

[89] APEC: see Program Requirements, p.8

[90] APEC: see Privacy Framework, part iii, Principle VII, 22, p.21; Program Requirements, Q28, 30, 35(a), pp.18-20

14. Transparency and Information Right / Notice

Common Elements Required for both BCR Approval and CBPR Certification

The organization must make a privacy statement readily available to every data subject before or at the time of collection [91]. This statement shall describe:

- How the data subjects are informed of the transfer and processing of their personal data [92];
- The identity of the controller(s) and of his representatives, if any and a contact point [93];
- The intended purposes for processing collected data [94];
- Any further information such as:
  i. the recipients or categories of recipients of the data [95];
  ii. the existence of the right of access to and the right to rectify the data concerning him/her, as well as how data subjects can get access to their personal data [96];

Where the data have not been obtained from the data subject, there are circumstances where the obligation to inform the data subject may not apply [97]. Such exemptions differ in the BCR and CBPR. Program-specific requirements for BCR and for CBPR shall be specified in an organization's personal data protection and privacy rules.

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
Further information shall be provided to data subjects insofar as such information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject [98]. Where the data have not been obtained from the data subject, the obligation to inform the data subject does not apply if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law [99]. While the obligation to inform the data subject may not apply in the circumstance above, it is not displaced on grounds of obviousness, nor that the personal data being processed is publicly available, nor that informing the data subject is technologically impracticable, nor only on the ground that the personal data was received from a third party.	The organization must also inform data subjects how the data are being collected and whether they are collected from [100]: - Directly from the individual; or - From third parties collecting on the controller's behalf; or - Other (must be described). There are circumstances where notice may not be necessary or practical [101]: - Obviousness; - Collection of Publicly-Available Information; - Technological Impracticability; - Disclosure to a government institution which has made a request for the information with lawful authority; - Disclosure to a third party pursuant to a lawful form of process;

	- Third-Party Receipt; - For legitimate investigation purposes; - Action in the event of an emergency. Additional information to be given to data subjects: - The fact that personal data is being collected [102]; - The purposes for which the data are made available to third parties [103]; - Information regarding the use and disclosure of data subjects' data [104]; - The choice and means offered to data subjects for limiting the use and disclosure of their personal data [105].

References

[91] EU: see Directive 95/46, art 10 and 11; WP153, point 1.7, p.5; WP74, point 5.7, p.19; WP154, point 7, p.5; APEC: see Privacy Framework, part iii, Principle II, 15 and 16, pp.12-13 and 16, p.13

[92] EU: see WP74, point 5.7, p.19; WP153, point 6.1.i, p.10; APEC: see Intake questionnaire, Q1, p.4; Q17-19, pp.10-11

[93] EU: see WP154, point 7, p.5; APEC: see Intake questionnaire, Q1-d), pp.4-5

[94] EU: see WP154, point 7, p.5; APEC: see Intake questionnaire, Q1-b) and Q3, pp.4-5

[95] EU: see WP154, point 7, p.5; APEC: see Privacy Framework, part iii, Principle II, 15-c), p.12

[96] EU: see WP154, point 7, p.5; APEC: see Privacy Framework, part iii, Principle II, 15-e), p.12; Intake Questionnaire, Q38- a), p.18

[97] EU: see Directive 95/46, art. 10 and 11; APEC: see Intake questionnaire, Qualifications to the Provision of Notice, p.6

[98] EU: see Directive 95/46, art. 10

[99] EU: see Directive 95/46, art. 11

[100] APEC: see Intake questionnaire, Q1-a), p.4 and Q5, p.7

[101] APEC: see Intake questionnaire, Qualifications to the Provision of Notice, p.6

[102] APEC: see Privacy Framework, part iii, Principle II, 15-a), p.12

[103] APEC: see Intake questionnaire, Q1-c), p.4

[104] APEC: see Intake questionnaire, Q1-e), p.5

[105] APEC: see Privacy Framework, part iii, Principle II, 15-e), p.12; Intake questionnaire, Q15-16, p.10

15. Rights of Access, Rectification, Erasure and Blocking of Data/Access and Correction

Common Elements Required for both BCR Approval and CBPR Certification

The organization must ensure that [106]:

- Every data subject shall be able to obtain from the controller confirmation of whether or not the controller holds personal data about him/her [107]:
- Every data subject shall be able to obtain a copy of all data relating to him/her held by the organization. The relevant data must be provided without constraint, within a reasonable time, and for a non-excessive fee (if any) [108];
- Every data subject shall be able to require a data controller to rectify or erase data which are in particular incomplete or inaccurate [109].

These obligations are subject to exemptions and qualifications according to applicable laws [110].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
The elements listed in the common referential above are rights granted to data subjects. An organization's personal data protection and privacy rules must also ensure that every data subject has the right to require a data controller to block data, in particular where the data are incomplete or inaccurate [111].	Controllers shall take steps to confirm the identity of the data subject requesting access [112]. When information is provided to a data subject who has exercised his/her access right, information shall be communicated in a reasonable manner that is generally understandable, and in a way that is compatible with the regular form of interaction with the individual [113]. A commitment that corrections or deletions shall be done within a reasonable timeframe [114]. Controllers shall provide a copy of the corrected personal data or provide confirmation that the data has been corrected or deleted to the data subjects [115]. Controllers shall provide the data subjects with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction [116].
Exceptions to Access Rights (BCR) EU national data protection laws may provide	**Exceptions to Access Requests (CBPR)** There are circumstances in which it may be

for some exceptions to the data subjects' access right, based on EU national law and to be interpreted in a restrictive way, in which cases it may be necessary for organizations to deny access requests to safeguard EU Member States' [117]: a) National security; b) Defense; c) Public security; d) The prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; e) An important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; f) A monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in c), d) and e); g) the protection of the data subject or of the rights and freedoms of others. EU national data protection laws may provide that, subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, the data subjects' right of access may, where there is clearly no risk of breaching the privacy of the data subject, be restricted when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.	necessary for organizations to deny access requests [118]: - Disproportionate burden; - Protection of confidential information; - Third Party Risk.

References

[106] EU: see Directive 95/46, art. 12; WP153, point 6.1.v., p.10; WP108, point 8.2.5, p.8

[107] APEC: see Privacy Framework, part iii, Principle VIII, 23-a), p.22; Intake questionnaire, Q36, p.17

[108] APEC: see Privacy Framework, part iii, Principle VIII, 23-b), p.22, Intake questionnaire, Q37, 37-b, 37-e), pp.17-18

[109] APEC: see Privacy Framework, part iii, Principle VIII, 23-c), p.22; Intake questionnaire, Q38, 38-b, pp.18-19

[110] EU: see Directive 95/46, art. 13; APEC: see Intake questionnaire, Qualifications to the Provision of Access and Correction Mechanisms, pp.19-20

[111] EU: see Directive 95/46, art. 12

[112] APEC: see Intake questionnaire, Q37-a), p.17

[113] APEC: see Intake questionnaire, Q37-c) and d), p.18

[114] APEC: see Intake questionnaire, Q38-a), p.19

[115] APEC: see Intake questionnaire, Q38-d), p.19

[116] APEC: see Privacy Framework, part iii, Principle VIII, 25, p.24, Intake questionnaire, Q38-e), p.19

[117] EU: see Directive 95/46, art. 13

[118] APEC: see Intake questionnaire, Qualifications to the Provision of Access and Correction Mechanisms, pp.19-20

16. Right to Object / Choice

Common Elements Required for both BCR Approval and CBPR Certification

Where appropriate or otherwise required by applicable law, the organization must ensure that the data subject shall be able to object to the processing of his/her personal data or to choose not to be subject to processing of his/her personal data, according to applicable laws [119].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules must also ensure that every data subject has the right to object to data processing of their personal data, as it is a right granted to data subjects. The right to object may be exercised by data subjects at any time. In particular, every data subject has the right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, and to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.	N/A
Exceptions to Right to Object (BCR) N/A	**Exceptions to Choice (CBPR)** There are circumstances in which it may not be necessary or practical for organizations to provide choice mechanisms to individuals [120]: - Obviousness; - Collection of Publicly-Available Information; - Technological Impracticability; - Third-Party Receipt; - Disclosure to a government institution which has made a request for the

	information with lawful authority; - Disclosure to a third party pursuant to a lawful form of process; - For legitimate investigation purposes; - Action in the event of an emergency.
Clarification of the Right to Object (BCR) A data subject has always the right to withdraw his/her consent. In addition, where there is another legal basis legitimating the processing, the data subjects may still object. Furthermore, EU national data protection laws provide for the circumstances in which data subjects may, at least where the legal basis of processing is derived from Article 7(e) or (f) of Directive 95/46/EC, object on compelling legitimate grounds relating to their particular situation, save where otherwise provided by EU Member States' national legislation. Where the objection is justified, the processing instigated by the controller may no longer involve those data [121]. The right to object cannot be displaced by grounds of obviousness, nor that the personal data being processed is publicly available, nor that the right to object is technologically impracticable, nor that the personal data was received from a third party.	**Clarification of Choice (CBPR)** Organizations are required to provide individuals with choice mechanisms as regards the collection, use and disclosure of their personal information [122].

References

[119] EU: see Directive 95/46, art. 14, WP153, point 6.1.v, p.10; WP108, point 8.2.5, p.8; APEC: see Intake questionnaire, Q14-16

[120] APEC: see Intake questionnaire, Qualifications to the Provision of Choice Mechanisms, pp.11-12

[121] EU: see Directive 95/46, art. 14

[122] APEC: see Program Requirements, Q14 to 16, pp. 11-13

17. Automated Individual Decisions

Common Elements Required for both BCR Approval and CBPR Certification

N/A

Elements Required for BCR Approval	Elements Required for CBPR Certification
An organization's personal data protection and privacy rules shall contain a commitment that no evaluation of or decision about the data subject which significantly affects him/her will be based solely on automated processing of their data unless that decision [123]: - is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or - is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.	N/A

References

[123] EU: see WP154, point 9, p.6

18. Security and Confidentiality

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall contain a requirement that appropriate technical and organizational measures to protect personal data have been implemented against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing [124].

Such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected [125].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also contain a requirement that security measures be implemented having regard to the state of the art and the cost of their implementation [126].	An organization's personal data protection and privacy rules shall also contain a requirement that security safeguards should be subject to periodic review and reassessment [127]. A policy on information security [128] and a policy for secure disposal of personal data shall be implemented [129]. Safeguards shall be implemented to detect, prevent, and respond to attacks, intrusions or other security failures [130]. Employees shall also be aware of the importance of, and obligations respecting, maintaining the security of personal data through regular training and oversight as demonstrated by procedures [131].

References

[124] EU: see Directive 95/46, art.17.1; WP108, point 8.2.4, p.8; APEC: see Privacy Framework, part iii, Principle VII, 22, p.2; Intake questionnaire, Q27, p.14

[125] EU: see Directive 95/46, art.17.1; APEC: see Privacy Framework, part iii, Principle VII, 22, p.21, Intake questionnaire, Q28, p.14

[126] EU: see Directive 95/46, art.17.1

[127] APEC: see Privacy Framework, part iii, Principle VII, 22, p.21

[128] APEC: see Intake questionnaire, Q26, p.14

[129] APEC: see Intake questionnaire, Q31, p.15

[130] APEC: see Intake questionnaire, Q32 and 33, p.15

[131] APEC: see Intake questionnaire, Q29 and 30-a), p.14

19. Training Program

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall provide for appropriate training on the organization's personal data protection and privacy rules for its personnel [132].

Additional Elements Required for BCR Approval	Additional Elements Required for CBPR Certification
The training requirement concerns employees who have permanent or regular access to personal data, are involved in the collection of personal data or in the development of tools used to process personal data [133].	Training shall cover privacy policies and procedures, including how to respond to privacy-related complaints [134]. Employees shall also be aware of the importance of, and obligations respecting, maintaining the security of personal data through regular training and oversight as demonstrated by procedures [135].

References

[132] EU: see WP74, point 5.1, p.16; APEC: see Intake questionnaire, Q44, p.22

[133] EU: see WP153, point 2.1, p.5

[134] APEC: see Program requirements, Q44, pp.25-26

[135] APEC: see Intake questionnaire, Q30-a), p.14

20. Monitoring and Audit Program

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall provide for monitoring of the application of and compliance with the organization's personal data protection and privacy rules [136].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also contain an obligation to audit the group's compliance with the personal data protection and privacy rules and in particular that [137]: - The audit program covers all aspects of the organization's personal data protection and privacy rules including methods of ensuring that corrective actions will take place. - Such audit must be carried out on a regular basis (specify the time) by the internal or external accredited audit team or on specific request from the privacy officer/function (or any other competent function in the organization). - The results of all audits should be communicated to the privacy officer/function (or any other competent function in the organization) and to the board of management. - The DPAs in the EU can receive a copy of such audits upon request. - The audit plan should allow the DPAs in the EU to have the power to carry out a data protection audit if required. - Each Member of the Group shall accept that they may be audited by the DPAs in the EU and that they will abide by the advice of the DPAs in the EU on any issue related to those rules.	An organization's personal data protection and privacy rules shall also contain the requirement that the controller attests on an annual basis to the continuing adherence to the CBPR program requirements [138]. Regular comprehensive reviews will be carried out by APEC Accountability Agents to ensure the integrity of the re-certification [139]. The controller shall carry out regular spot checking or monitoring of his/her personal data processors, agents, contractors or other service providers to ensure compliance with his/her instructions and/or agreements/contracts [140].

References

[136] EU: see WP74, point 5.2, p.16; APEC: see Recognition application, Annex A, 6-8, p.6

[137] EU: see WP153, point 2.3, p.7

[138] APEC: see Recognition application, Annex A, 8, p.6

[139] APEC: see Recognition application, Annex A, 8, p.6

[140] APEC: see Intake questionnaire, Q49, p.23

21. Compliance and Supervision of Compliance

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall provide for the appointment of appropriate staff (such as a network of privacy officers) to oversee and ensure compliance with the organization's personal data protection and privacy rules [141].

Additional Elements Required for BCR Approval [142]	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also contain a brief description of the internal structure, role and responsibilities of the network or privacy officers or similar function created to ensure compliance with the organization's personal data protection and privacy rules. The appropriate staff appointed shall be supported by top management. Example of internal structure, role and responsibilities of the network or privacy officers or similar function created to ensure compliance with the organization's personal data protection and privacy rules: the chief privacy officer advises the board of management, deals with investigations by national DPAs in the EU, annually reports on compliance, ensures compliance at a global level and that privacy officers can be responsible for handling local complaints from data subjects, reporting major privacy issues to the chief privacy officer and for ensuring compliance at a local level.	An organization's personal data protection and privacy rules shall also contain a requirement that the appointed individual(s) shall implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable [143].

References

[141] EU: see WP74, point 5.1, p.16; APEC: see Intake questionnaire, Q40, p.21

[142] EU: see WP153, point 2.4, p.8

[143] APEC: see Program requirements, Q40, pp.24-25

22. Internal Complaint Mechanisms

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall put in place a complaint handling process where [144]:

- Any data subject may complain that any member of the Group is not complying with the organization's personal data protection and privacy rules;
- The complaints will be dealt with by a clearly identified department/person.

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
The identified department/person who handles complaints must benefit from an appropriate level of independence in the exercise of his/her functions [145].	When responding to data subjects about their complaints, a commitment that this response includes an explanation of remedial action relating to their complaints [146].

References

[144] EU: see WP74, point 5.3, p.17; APEC: see Intake questionnaire, Q41-42, p.21

[145] EU: see WP74, point 5.3, p.17

[146] APEC: see Intake questionnaire, Q43, p.21

23. Updates to an Organization's Personal Data Protection and Privacy Rules

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall provide for the reporting of any significant changes to the organization's personal data protection and privacy rules or to the list of members, to all Group members, as well as the DPAs in the EU and APEC Accountability Agents, to take into account modifications of the regulatory environment and the company structure and more precisely that some modifications might require a new authorization from the national DPAs in the EU and/or trigger a review by APEC Accountability Agents [147].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall also contain a commitment that substantial modifications to the organization's personal data protection and privacy rules will also be communicated to the data subjects [148]. Updates to the organization's personal data protection and privacy rules or to the list of the Members of the Group bound by the organization's personal data protection and privacy rules are possible without having to re-apply for an authorization providing that [149]: i) An identified person keeps a fully updated list of the members of the Group and keeps track of and record any updates to the organization's personal data protection and privacy rules and provide the necessary information to the data subjects and to national DPAs in the EU upon request. ii) No transfer is made to a new member until the new member is effectively bound by the organization's personal data protection and privacy rules and can deliver compliance. iii) Any changes to the organization's personal data protection and privacy rules or to the list of Members should be reported once a year to the national	An organization's personal data protection and privacy rules shall also contain a requirement that where there has been a material change to the organization's personal data protection and privacy rules (as reasonably determined by the APEC Accountability Agent in good faith), an immediate review process will be carried out by the Accountability Agent [150]. Organizations should provide an up-to-date statement about their practices and policies with respect to personal information [151]. In addition, organizations are required to provide individuals with choice mechanisms as regards the collection, use and disclosure of their personal information [152].

DPAs in the EU granting the authorizations with a brief explanation of the reasons justifying the update.	

References

[147] EU: see WP74, point 4.2, p.15; APEC: see Recognition application, Annex A, 8, p.6

[148] EU: see WP154, point 21, pp.9-10

[149] EU: see WP74, point 4.2, p.15

[150] APEC: see Recognition application, Annex A, 8, p.6

[151] APEC: see Privacy Framework, part iii, Principle II, 15; Intake questionnaire, Q1, p.4

[152] APEC: see Program Requirements, Q14 to 16, pp. 11-13

24. Actions in Case of Risk of Local Legislation Preventing Compliance with the Organization's Personal Data Protection and Privacy Rules and in Case of Requests for Access by Law Enforcement Authorities

Common Elements Required for both BCR Approval and CBPR Certification

N/A

Elements Required for BCR Approval [153]	**Elements Required for CBPR Certification**
An organization's personal data protection and privacy rules shall contain a clear provision indicating that where a member of the Group has reasons to believe that the legislation applicable to him prevents it from fulfilling its obligations under the organization's personal data protection and privacy rules and has substantial effect on the guarantees provided therein, this member shall promptly inform the EU headquarters or the EU member with delegated data protection responsibilities or the other relevant privacy function (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In addition, an organization's personal data protection and privacy rules shall provide for that where there is conflict between national law and the obligations, requirements and undertakings in the organization's personal data protection and privacy rules of the EU headquarters, the EU member with delegated data protection responsibilities or the other relevant Privacy Function have to consult the competent national DPAs in the EU and have to take a responsible decision on what action to take. Any incidents under this point of the organization's personal data protection and privacy rules will be detailed and reviewed by the regular audits mentioned in section 20.	An organization's personal data protection and privacy rules shall contain a requirement that there is a procedure in place to cover situations of judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal data [154].

References

[153] EU: see WP74, point 3.3.3, pp.13-14 and WP154, point 16, p. 8

[154] APEC: see Intake questionnaire, Q45, p.22

25. Mutual Assistance and Co-operation with National DPAs in the EU / APEC PEAs

Common Elements Required for both BCR Approval and CBPR Certification

N/A

Elements Required for BCR Approval	Elements Required for CBPR Certification
An organization's personal data protection and privacy rules shall contain an obligation on [155]: - Members of the Group to cooperate and assist each other to handle a request or complaint from an individual or an investigation or inquiry by DPAs in the EU. - Entities to abide by the advice of the national DPAs in the EU on any issues regarding the interpretation of the organization's personal data protection and privacy rules.	Organizations from participating economies may receive CBPR certification. Member Economies may only participate in the CBPR system if their Privacy Enforcement Authority (PEA) is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA) [156].

References

[155] EU: see WP74, point 5.4, p.17

[156] APEC: see JOP Charter, paragraph 2.2i, p. 15

26. Relationship between Local Laws and the Organization's Personal Data Protection and Privacy Rules

Common Elements Required for both BCR Approval and CBPR Certification

N/A

Elements Required for BCR Approval	**Elements Required for CBPR Certification**
Where personal data is processed in the EU, EU data protection law must be applied. An organization's personal data protection and privacy rules shall therefore confirm that [157]: - Where the local legislation, for instance EU legislation, requires a higher level of protection for personal data it will take precedence over the organization's personal data protection and privacy rules. - In any event data shall be processed in accordance with the law of the relevant Member State as provided by Article 4 of the Directive 95/46/EC.	N/A
Clarification of Relationship between Local Laws and BCR N/A	**Clarification of Relationship between Local Laws and CBPR** [158] Participation in the CBPR system does not replace a participating organization's domestic legal obligations. Where there are no applicable domestic privacy protection requirements in an Economy, the organization's personal data protection and privacy rules are intended to provide a minimum level of protection. Where domestic legal requirements exceed what is expected in the organization's personal data protection and privacy rules, the full extent of such domestic law and regulation will continue to apply. Where requirements of the organization's personal data protection and privacy rules exceed the requirements of domestic law and regulation, the organization will need to carry

	out such additional requirements in order to participate. Nonetheless, Privacy Enforcement Authorities in that Economy should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR requirements.

References

[157] EU: see WP74, point 3.3.3, pp.13-14

[158] APEC: see Policies, Rules and Guidelines, paragraphs 43 and 44, pp.10-11

27. Final Provisions

Common Elements Required for both BCR Approval and CBPR Certification

An organization's personal data protection and privacy rules shall specify their effective date [159].

References

[159] EU: see WP154, point 23, p.10; APEC: see Program requirements, Q1, p.2

Appendixes

Appendix 1. Documentation to be provided by an organization seeking approval of its BCR by the national DPAs in the EU and by an organization seeking certification of its CBPR by APEC Accountability Agents

Appendix 1. Documentation to be provided by an organization seeking approval of its BCR by the national DPAs in the EU and by an organization seeking certification of its CBPR by APEC Accountability Agents

An organization applying for approval of its BCR and for certification of its CBPR shall provide the national DPAs in the EU and the APEC Accountability Agent with any documentation that shows that obligations, requirements and commitments in the organization's personal data protection and privacy rules are being respected, for instance [160]:

- Privacy policies (e.g. Customer Privacy Policy, HR Privacy Policy) to inform data subjects (e.g. customers, employees) about the way the company protects their personal data [161];
- Guidelines for employees having access to personal data so that they can easily understand and apply the rules prescribed into the Privacy Rules (e.g. guidelines on how to respond to a complaint from a data subject, on how to provide information to data subjects, on appropriate security/confidentiality measures to be observed) [162];
- Examples and/or explanation of the training program [163];
- Description of the internal complaint system [164];
- Security policy for IT systems processing EU and APEC personal data [165];
- Any standard contracts to be used with data processors (members or non members of the Group) processing EU personal data and APEC personal data, as appropriate [166].

Additional Elements Required for BCR Approval	**Additional Elements Required for CBPR Certification**
The applicant organization shall also provide the national DPAs in the EU with: - A job description of data protection officers or other persons in charge of data protection in the company - Standard Application Form WP133 [167]. - Data protection audit plan and program defined with relevant persons (internal/external accredited auditors of the company). - Documentation showing that the member that is at the origin of the transfer of data outside of the EU and either the EU headquarters or the EU Member with delegated responsibilities has sufficient assets to enable payment of	The applicant organization shall also provide the APEC Accountability Agents with: - Intake questionnaire. - Examples of additional documentation that may be necessary for APEC Accountability Agents to carry out their review of the organization's personal data protection and privacy rules: - Examples of notices provided to data subjects [168]. - Documentation showing compliance with data collection limitation with identification of [169]: i) Each type of data collected; ii) The corresponding stated purpose of collection for each; and

compensation for damages resulting from the breach of the organization's personal data protection and privacy rules.	iii) All uses that apply to each type of data; iv) An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. - Documentation showing that personal data is collected, used and disclosed for identified purposes or other compatible or related purposes, unless permitted under specific circumstances [170]. - Documentation showing the mechanisms provided to data subjects so that they may exercise choice in relation to the collection, use and disclosure of their personal data; and showing that such mechanisms are in place and operational and that the purpose of collection is clearly stated [171]. - Procedures implemented to verify and ensure that the personal data held is up to date, accurate and complete, to the extent necessary for the purposes of use [172]. - Documentation showing the existence of agreements with processors, agents, contractors or other service providers, to ensure that the controller's obligations to data subjects will be met [173].

References

[160] EU: see WP154, Documentation to be provided to the DPAs, pp.10-11

[161] APEC: see Program requirements, Q1, pp.2-4

[162] APEC: see Program requirements, Q29, p.18; Q44, pp.25-26

[163] APEC: see Program requirements, Q44, pp.25-26

[164] APEC: see Program requirements, Q41-43, p.25

[165] APEC: see Program requirements, Q26, p.17; Q31, p.19

[166] APEC: see Program requirements, Q46, pp.26-27

[167] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc

[168] APEC: see Program requirements, Q2, p.4

[169] APEC: see Program requirements, Q6, p.6

[170] APEC: see Program requirements, Q8, p.8

[171] APEC: see Program requirements, Q14-17, pp.11-13

[172] APEC: see Program requirements, Q21, p.15

[173] APEC: see Program requirements, Q46-47, pp.26-27