This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

APEC Cross-Border Privacy Rules Requirements and EU-U.S. Privacy Shield Requirements Mapped to the Provisions of the UK General Data Protection Regulation

This document presents a comparison of the APEC Cross-Border Privacy Rules (CBPR) Requirements and the EU-U.S. Privacy Shield Requirements to the requirements of the UK General Data Protection Regulation (GDPR). For purposes of this analysis, the Centre for Information Policy Leadership (CIPL) at Hunton Andrews Kurth LLP analyzed relevant documents pertaining to participation in both the CBPR and Privacy Shield certification system.[1]

Below we present key recommendations, as well as the main findings from the results of this analysis, followed by two pie charts demonstrating the percentage overlap of the requirements of the CBPR and Privacy Shield Requirement to the UK GDPR. Following this is a detailed table containing the analysis.

This map does not refer to any additional data protection requirements found in the UK Data Protection Act of 2018 (DPA). Relevant DPA provisions that do not appear in the UK GDPR relate to the following issues:

- Special categories of personal data, criminal convictions data, etc.
- Automated decisions required or authorized by law.
- Conditions applicable to reliance on exemptions under Article 23.
- Processing for archiving, research and statistical purposes.
- Enforcement.
- Prohibitions and criminal offences.

[1] See Cross Border Privacy Rules System Documents available at http://cbprs.org/documents/. In particular, this analysis considered the CBPR Program Requirements, Intake Questionnaire, Policies, Rules and Guidelines and the Accountability Agent Application, and the Requirements of Participation in the Privacy Shield Program, available at https://www.privacyshield.gov/article?id=Requirements-of-Participation.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Main Findings from the Results of this Analysis

1. The requirements of the APEC CBPR System and the EU-U.S. Privacy Shield overlap significantly with the requirements of the UK GDPR at 61% and 67%, respectively. This overlap comprises requirements of the UK GDPR that appear either directly or indirectly within each system.

2. In cases where the requirements of the APEC CBPR System and the EU-U.S. Privacy Shield do not match to the requirements of the UK GDPR, this does not necessarily mean those instruments provide a lower level of protection with respect to such provisions/processing scenarios. Furthermore, in cases where there is a non-match with a GDPR provision that provides lesser protection to individuals (e.g. exemptions to obligations - see point 4. a. below), such non-matches may not need to be bridged with the CBPR system.

3. **CBPR matches and non-matches providing a higher level of protection.** With respect to some CBPR non-matches, the CBPR requirements actually provide a higher level of protection than that included in the GDPR. For example:

    a. ***Legitimate and public interest (GDPR Article 6(1)(e) and (f)) [CBPR non-match to GDPR]***: The CBPR do not include public interest or legitimate interests as legal bases for processing, unlike the GDPR. This has the effect of creating a more restrictive standard for processing under the CBPR that will not have to be augmented through any add-on requirements for purposes of bridging the requirements of the CBPR with those of the UK GDPR.

    b. ***Cooperation with the Commissioner (GDPR Article 31) [CBPR match to GDPR]***: The CBPR requires organizations to have procedures in place to respond to judicial or other government subpoenas, warrants or orders. In the context of cooperation with the Commissioner under Article 31 GDPR, the CBPR goes further with respect to responding to such requests by mandating specific procedures be put in place.

4. **CBPR non-matches that are not less protective.** Other CBPR non-matches do not necessarily indicate substantively less protection than that provided by the GDPR.

    a. ***Exemptions to notice to individuals where data has not been collected directly from them (GDPR Article 14)***: The CBPR do not contain notice requirements for organizations that collect information about individuals from sources other than

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the individuals themselves. Consequently, the CBPR does not contain exemptions to this requirement. However, the lack of exemptions here does not mean that this non-match must be bridged with the GDPR.

b. ***Icons (GDPR Article 12(7))***: There is no match to the GDPR transparency provision allowing icons but the absence of this does not mean that existing transparency requirements under the CBPR provide substantively less transparency when compared to the standards under the GDPR.

c. ***Exemption from obligation to maintain records (GDPR Article 30(5))***: There is no match to the GDPR provision exempting certain organizations from maintaining records. However, the absence of such an exemption does not mean that the CBPR provides less protection.

d. ***Publishing DPO contact details (GDPR Article 37(7))***: There is no match to the GDPR requirement to publish the contact details of the DPO and communicate them to the Commissioner but this does not necessarily mean that the CBPR is less protective. Under the CBPR applicants must still provide a "Contact Point" – regardless of whether this is a DPO or not.

e. ***Position of the DPO (GDPR Article 38)***: The GDPR requirements concerning the position of the DPO do not fully match with the requirements contained in the CBPR. Although some of the technicalities of the DPO position are spelled out in the GDPR, the CBPR still requires applicants to provide a "Contact Point" and to have an individual responsible for compliance, and the absence of the technicalities listed in the GDPR do not necessarily indicate that the CBPR is less protective in this regard.

f. ***Tasks of the DPO (GDPR Article 39)***: The GDPR spells out specific tasks that the DPO is responsible for. This list of tasks does not fully match with the requirements contained in the CBPR. However, this does not necessarily mean that the "Contact Point" or individual responsible for compliance under the CBPR will not undertake such obligations. As a result, the lack of these requirements in the CBPR does not necessarily mean that it provides less protection than the GDPR.

g. ***Administrative fines and penalties (GDPR Articles 83 and 84)***: Administrative fines and penalties as described in the GDPR are subject to the domestic law of the participating CBPR country and are enforceable by privacy enforcement authorities in those jurisdictions. As a result, such remedies are not specified in the CBPR program requirements.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

However, under the CBPR, the official DPAs in participating jurisdictions can impose their own set of sanctions, including administrative fines under their legal framework, including redress in court.

5. **CBPR non-matches that are less protective.** At the same time, other CBPR non-matches indicate lesser protection. In some cases, the CBPR does not include specific concepts contained in the GDPR (e.g. data portability), while in others the difference in protection results for different approaches to concepts contained in the GDPR.

    a. ***Publicly available data***: The CBPR generally do not apply to publicly available data that was made available to the public by the individual or that appears in public government records, journalistic reports or information required by law to be public.

    b. ***Children's data (GDPR Article 8)***: The CBPR does not contain requirements around obtaining parental consent for processing the data of children under a certain threshold age.

    c. ***Sensitive data (GDPR Article 9)***: The CBPR do not prohibit processing of sensitive data unless a special condition exists.

    d. ***Processing related to criminal convictions and offences (GDPR Article 10)***: The CBPR do not provide restrictions on processing data related to criminal convictions and offences.

    e. ***Notice to individuals where data has not been collected directly from them (GDPR Article 14)***: The CBPR do not contain notice requirements for organizations that collect information about individuals from sources other than the individuals themselves. Under the CBPR, individuals receive notice from controllers that collect their information directly and subsequently if the controller discloses that information for unrelated purposes.

    f. ***Informing other controllers that the data subject has requested erasure (GDPR Article 17(2))***: The CBPR do not require the communication of erasure requests to other third parties except in the limited circumstances whereby the controller is communicating a correction request to third parties, which might include deletion under the CBPR.

    g. ***The right to restrict processing (GDPR Article 18)***: The CBPR do not contain a right to restrict processing with respect to the specific scenarios outlined in the GDPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

h. ***The right to data portability (GDPR Article 20)***: The CBPR do not contain a right to data portability.

i. ***The right to object (GDPR Article 21)***: The CBPR do not contain a right to object to specific processing.

j. ***The right not to be subject to automated-decision making (GDPR Article 22)***: The CBPR does not contain a right not to be subject to solely automated-decision making producing legal or similarly significant effects.

k. ***Joint controllers (GDPR Article 26)***: The concept of joint controllers is not included in the CBPR.

l. ***Breach notification to the Commissioner (GDPR Article 33)***: There is no requirement to notify breaches to a supervisory authority under the CBPR.

m. ***Breach notification to individuals (GDPR Article 34)***: There is no requirement to notify breaches to individuals under the CBPR.

n. ***Data Protection Impact Assessment (DPIA) (GDPR Article 35)***: There is no requirement to carry out a DPIA under the CBPR.

o. ***Prior consultation (GDPR Article 36)***: There is no requirement to consult a supervisory authority where DPIAs indicate processing would result in a high risk (including because there is no requirement to conduct DPIAs in the first instance).

6. **CBPR non-matches that achieve the same objectives as the GDPR.** There are also some cases where CIPL considers there is a non-match/indirect match between the requirements of the CBPR and the UK GDPR that accomplishes the same goal as the provisions of the GDPR. In other words, the match does not correspond in the CBPR to every detail contained in the GDPR or the requirement may be expressed differently but the spirit of the law and outcome is the same:

   a. ***The right to erasure (GDPR Article 17)***: The right to erasure exists in the CBPR. However, the scope of this right is broader and more restrictive in the GDPR. The exceptions to the right to erasure contained in the GDPR are not expressly listed in the CBPR but the exceptions to providing correction (and by extension deletion under the CBPR) are similar in spirit to the GDPR exceptions for the right to erasure.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

b. ***Notification obligation regarding rectification/erasure/restriction (GDPR Article 19)***: The CBPR contains an obligation to communicate corrections to third parties to whom personal information was transferred/disclosed. This achieves the same objective as Article 19 of the GDPR with respect to rectification and, in limited ways, erasure. There is no right to restriction under the CBPR.

c. ***Restriction of obligations and rights (GDPR Article 23)***: The CBPR provides qualifications to the provision of certain obligations and rights which achieves a similar outcome to Article 23 of the GDPR. However, the GDPR is broader in this regard as it is the Secretary of State who has discretion to impose further restrictions on obligations/rights.

d. ***Privacy by Design (GDPR Article 25)***: There is no explicit privacy by design or by default requirement in the CBPR. However, the CBPR accountability and security safeguards and provisions around uses of personal information overlap with the spirit of the GDPR privacy by design provisions.

e. ***Commitment to confidentiality regarding processor contracts (GDPR Article 28(3)(b))***: Under the CBPR, any confidentiality obligations that are included in processor contracts will attach to persons authorized to process data by the processor entity which achieves the same outcome as Article 28(3)(b) of the GDPR.

f. ***Subprocessor agreements (GDPR Article 28(4))***: Under the CBPR, protections generally flow with the data. For example, an applicant must limit the use of collected information to the intended purpose, including when disclosing data to third parties for processing. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations on processing apply to the processor, who, in turn, is bound by them and cannot onward transfer without these protections. Moreover, under the CBPR, the Applicant may require a processor to obtain the controller's consent to subprocessing. In such cases, the applicant will likely require that sub-processor to adhere to the same requirements as the processor the applicant initially engaged. This achieves the same outcome as Article 28(4) of the GDPR.

g. ***Provision of records to enforcement authority (GDPR Article 30(4))***: Under the CBPR, certified organizations must participate in any dispute resolution requested by a consumer or the Accountability Agent and presumably provide records in the process. Moreover, certified organizations are subject to the jurisdiction of the Privacy Enforcement Authority in the jurisdiction in which they were certified and must respond to document requests from the Privacy

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Enforcement Authority in the context of an investigation. This achieves the same objective as the obligation to make records available to the Commissioner on request under the GDPR.

h. ***GDPR Onward Transfer Requirements (See GDPR Articles 44, 45 and 46)***: While the CBPR requirements do not map to the general cross-border transfer requirements in the GDPR (because the CBPR are a transfer mechanism) the CBPR directly and implicitly provide onward transfer safeguards that achieve similar protections as the GDPR.

i. ***Fines (GDPR Article 83)***: While the CBPR does not spell out levels of fines or circumstances under which they apply, the Accountability Agent has a range of options in enforcing the CBPR program requirements where the certified organization has failed to remedy a violation as ordered by an Accountability Agent, including by issuing a "monetary penalty". This provides the same enforcement remedy as under the GDPR (see note on enforcement under CBPR below).

7. Some elements of the EU GDPR are contained in the CBPR but not in the EU-U.S. Privacy Shield. For example:

a. ***Notification obligation regarding rectification/erasure/restriction (GDPR Article 19)***: The CBPR contains an obligation to communicate corrections to third parties to whom personal information was transferred/disclosed. The Privacy Shield does not contain such a requirement.

b. ***DPO Appointment (GDPR Article 37)***: There is no requirement to appoint a DPO under the Privacy Shield. Under the CBPR, applicants must provide a "Contact Point" and designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles, including as described in its Privacy Statement.

8. APEC also developed a **Privacy Recognition for Processors (PRP)**. It is a streamlined certification for processors with respect to the security safeguards and accountability measures that enable processors to process personal data on behalf of controllers consistent with applicable CBPR obligations and/or the requirements specified by the controllers. The security and accountability measures largely track the corresponding requirements in the CBPR, but are expressly articulated from the processors perspective and more detailed. The PRP system is not part of the CBPR and only two of the CBPR countries are also participating in the PRP. While processors can and do currently certify to the CBPR, processor-specific requirements are more clearly articulated in the PRP and many CBPR requirements simply would not be relevant to processors and certified processors would not have to implement or comply with them.

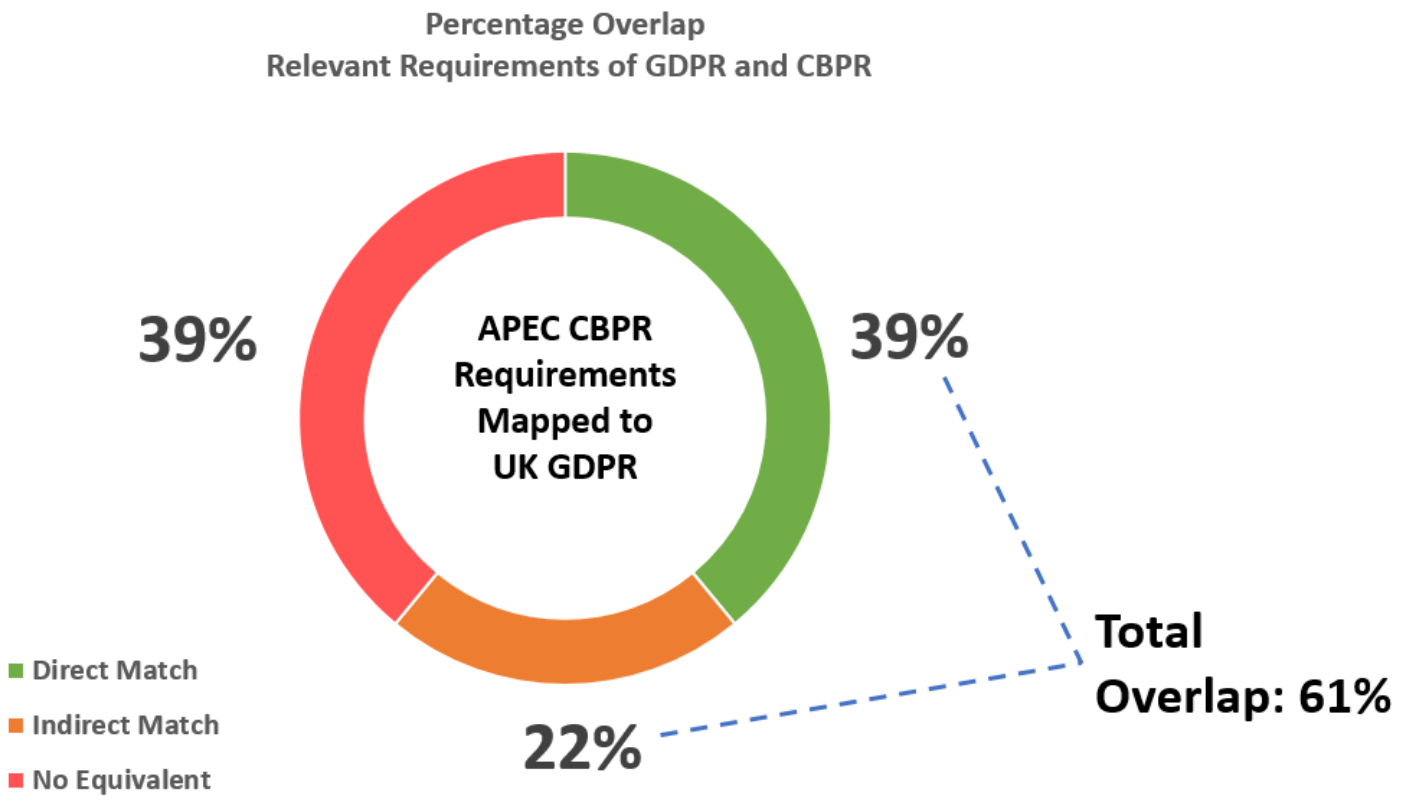
This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Note on the Enforceability of the APEC CBPR System

Once an organization joins the system and is certified by a third-party Accountability Agent under the CBPR Program Requirements, the certification becomes legally enforceable by the Privacy Enforcement Authority (PEA) in the economy in which the organization has been certified. To join the CBPR system, APEC economies must demonstrate that the CBPR are enforceable under their laws and by their PEA. Enforcement of the CBPR is currently provided by APEC-based Privacy Enforcement Authorities that have joined the APEC Cross-Border Privacy Enforcement Arrangement (CPEA). If the CBPR were to be globalized, the CPEA would have to be expanded to allow participation by PEAs from non-APEC economies. Organizations can certify to the CBPR only if they are subject to the enforcement jurisdiction of the PEA in the economy in which they seek certification.

With respect to the sanctions and fines for violations, as mentioned above, administrative fines and penalties as described in the GDPR are subject to the domestic law of the participating CBPR country and are enforceable by privacy enforcement authorities in those jurisdictions. As a result, such remedies are not specified in the CBPR program requirements. Under the CBPR, judicial redress and administrative fines and remedies are left to the individual jurisdictions. The PEAs in the participating jurisdictions can impose their own set of available sanctions, including any administrative fines provided under their legal framework.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

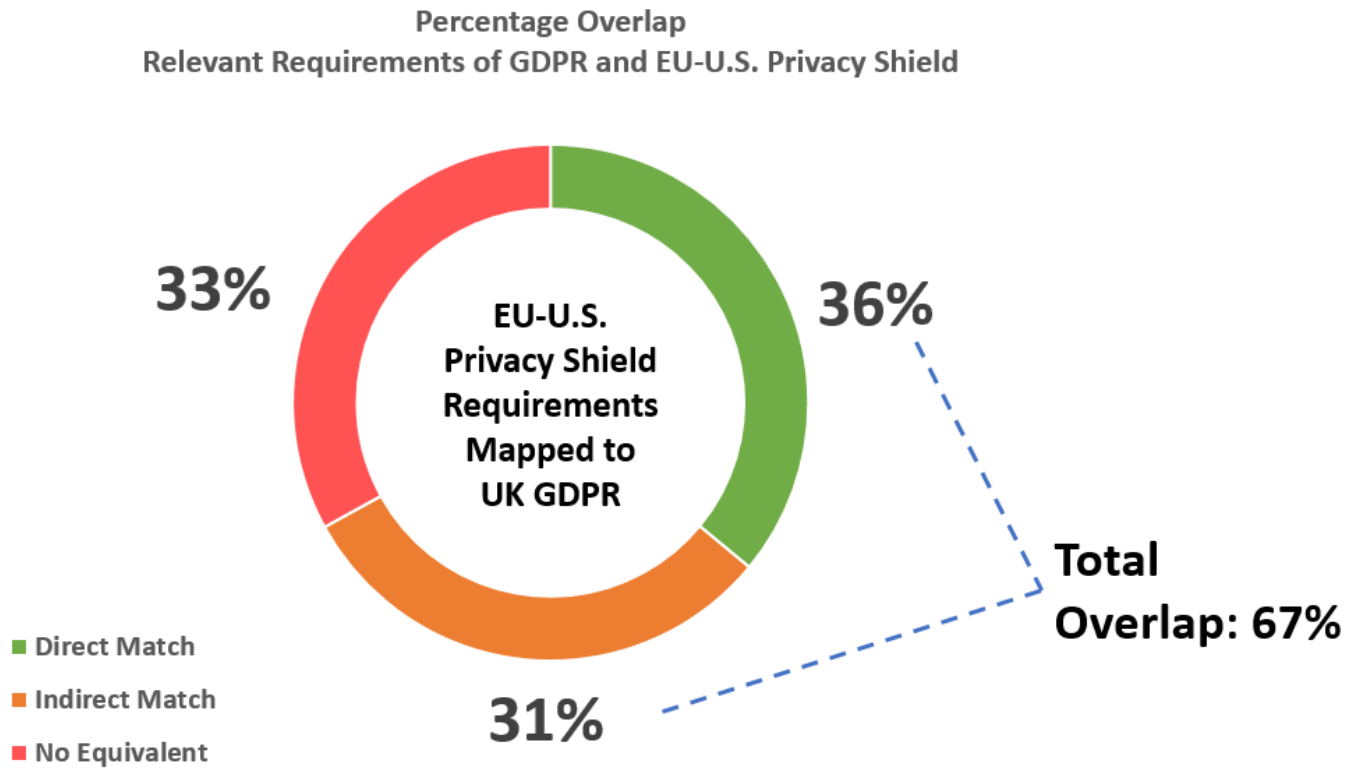


This chart compares 138 relevant GDPR requirements against the requirements of the APEC Cross-Border privacy rules.

In terms of the percentage overlap:

- **61% of requirements (84 requirements) contained in the GDPR appear either directly or indirectly within the CBPR system.**
- **39% of GDPR requirements (54 requirements) do not appear in the CBPR. This figure does not indicate that the CBPR requirements are 31% less protective as explained above.**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.



This chart compares 141 relevant GDPR requirements against the requirements of the EU-U.S. Privacy Shield.

In terms of the percentage overlap:

- **67% of requirements (94 requirements) contained in the GDPR appear either directly or indirectly within the Privacy Shield.**
- **31% of GDPR requirements (54 requirements) do not appear in the Privacy Shield. This figure does not indicate that the Privacy Shield requirements are 31% less protective as described above.**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Detailed Mapping Analysis

Table Legend:

	Table Headings
	UK GDPR provision has an equivalent match in the APEC CBPR / EU-U.S. Privacy Shield
	UK GDPR provision does not have an equivalent match in the APEC CBPR / EU-U.S. Privacy Shield
	UK GDPR provision has a similar/implied but not direct equivalent match in the APEC CBPR / EU-U.S. Privacy Shield
	UK GDPR provision
	Overarching UK GDPR provision (e.g. Article 5) with sub-provisions following in the chart (e.g. 5(1)(a))
	UK GDPR provisions that are not relevant to this mapping exercise
	EU GDPR provisions that have been deleted from the UK GDPR (as indicated by the UK GDPR Keeling Schedule)
FFD	FFD = For further discussion. Indicates areas of overlap that might be subject to multiple interpretations

Note that for purposes of the APEC CBPR Requirements, "**applicant**" means the data controller (although it may also include the data processor as such entities can also certify to the CBPR system). For purposes of this mapping exercise, we use the term applicant to mean the controller.

EU-U.S. Privacy Shield Requirements	UK GDPR Article		APEC CBPR Requirements	Comments
EU-U.S. Privacy Shield Framework Overview • *Lays down the rules relating to the protection of personal data transferred to the U.S. from the EU.*	1	**Subject matter and objectives** • *Lays down rules relating to the protection of personal data.*	**Intake Questionnaire; General (iv.) personal information** • *Applicant must specify what type(s) of personal information it is applying for certification? (customer, employee, prospective*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			customer/employee or other).	
EU-U.S. Privacy Shield Framework Overview • *Privacy Shield applies to U.S. organizations that self-certify their adherence to the Privacy Shield Principles.*	2	**Material scope** • *Applies to automated/structured processing of personal data.* • *Sets out exceptions to which the Regulation does not apply.*	**Intake Questionnaire; General (i) & (ii);** • *CBPR certification applies to applicant organization and listed subsidiaries/affiliates* • *Publicly available information is not covered by the CBPR (see Qualifications to the Provision of Notice and Choice Mechanisms in the intake questionnaire).* • *CBPR certification only applies to commercial information – by inference, CBPR does not apply to law enforcement or intelligence activities or processing conducted for purely personal or household activities.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Framework Overview *In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the U.S. FTC, U.S. Department of Transportation, or another statutory body that will effectively ensure compliance with the Principles; (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement the Principles.*	3	**Territorial scope** • *Sets out scenarios regarding the jurisdictional scope and extraterritorial reach of the Regulation.*	**Intake Questionnaire; General** • *Applicant must specify which economies it or its affiliates/subsidiaries collect or anticipate collecting and transfer or anticipate transferring personal information to be certified under the CBPR.*	
EU-U.S. Privacy Shield I. Overview • *"Personal data" and "personal information" are data about an identified or identifiable*	4	**Definitions** • *"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable*	**Definitions in the APEC Privacy Framework** • *The CBPR were developed specifically to implement the Privacy Principles of the APEC Privacy*	Note that the CBPR generally do not apply to publicly available data that was made available to the public by the individual or that appears in public government records,

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form. • *"Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.* • *"Controller" means a person or organization which, alone or jointly with others, determines*		*natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.* • *"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,*	*Framework. The relevant definitions for the CBPR (e.g. "personal information", "personal information controller") are found in the APEC Privacy Framework.* • *"Personal information" is defined under Part II of the Framework as any information about an identified or identifiable individual.* • *"Personal information controller" is defined as a person or organization who controls the collection, holding, processing or use of personal information.*	journalistic reports or information required by law to be public.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the purposes and means of the processing of personal data.		*restriction, erasure or destruction.* • *"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.* • *See the full text of the UK GDPR for the many other definitions contained in Article 4.*		
	5	**Principles relating to processing of personal data**		
EU-U.S. Privacy Shield Framework Overview • *Consistent with the goal of enhancing privacy protection, organizations should strive to implement the Privacy Shield Principles fully and transparently,*	5(1)(a)	*Lawfulness, fairness and transparency* • *Personal data shall be processed lawfully, fairly and in a transparent manner.*	**CBPR Program Requirements; Assessment Criteria 7** • *Applicant must collect personal information by lawful and fair means, consistent with the requirements of the jurisdiction that governs*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

including indicating in their privacy policies where exceptions will apply on a regular basis.			*the collection of such personal information.*	
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Personal information must be limited to the information that is relevant for the purposes of processing.* • *An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual.*	5(1)(b)	*Purpose limitation* • *Personal data shall be collected for specified, explicit and legitimate purposes and not further incompatibly processed.*	**CBPR Program Requirements; Assessment Criteria 6, 8, 10, 12 & 13** • *Applicant must limit the use of collected personal information to those purposes for which the information was collected or for other compatible or related purposes.* • *If applicant discloses personal information to other personal information controllers, the disclosure must be limited to the purpose of collection of compatible or related purposes unless new purposes of processing have been consented to by the individual, it is*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfers • *Where data is transferred to a third party acting as a controller, the transferring organization must enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it*			*necessary to disclose the data to provide a service or product requested by the individual or disclosure is compelled by law.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

can no longer meet this obligation.				
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Personal information must be limited to the information that is relevant for the purpose of processing.*	5(1)(c)	*Data minimization* • *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*	**CBPR Program Requirements; Assessment Criteria 6** • *Applicant must limit the amount and type of personal information collected to that which is relevant to the stated purpose. Proportionality may be a factor in determining what is relevant (see assessment purpose).*	
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *An organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current.*	5(1)(d)	*Accuracy* • *Personal data shall be accurate and, where necessary, kept up to date.*	**CBPR Program Requirements; Assessment Criteria 21 and 22** • *Applicant must take steps to verify that the personal information it holds is up to date, accurate and complete, including by having a mechanism for correcting inaccurate, incomplete and outdated personal information to the extent necessary for purposes of its use.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Personal information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a (Purpose Limitation – see above).*	5(1)(e)	*Storage limitation* • *Personal data shall be kept no longer than necessary.*	**No Direct Equivalent in CBPR**	Indirectly implied via requirement 31 – applicant must implement a policy for secure disposal of information. A storage limitation period may form part of a secure disposal policy. Moreover, the nature of an end to end data security requirement implies that data should not be held in perpetuity unless there is a significant reason for doing so.
EU-U.S. Privacy Shield Principle 4. Security • *Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking*	5(1)(f)	*Integrity and confidentiality* • *Personal data shall be processed in a manner that ensures appropriate security of the personal data.*	**CBPR Program Requirements; Assessment Criteria 30(b)** • *Applicant must implement safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of information and the context in which it is held through information systems and management, including network and software*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

into due account the risks involved in the processing and the nature of the personal data.			*design, as well as information processing, storage, transmission and disposal.*	
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles. This can be done either through self-assessment or outside compliance reviews, both of which are described in further*	5(2)	*Accountability* • *The controller shall be responsible for, and be able to demonstrate compliance with, the processing principles.*	**CBPR Program Requirements; Assessment Criteria 39** • *Applicant must have measures to ensure compliance with the CBPR program requirements (i.e. internal guidelines or policies, contracts, compliance with applicable industry or sector laws and regulations, compliance with self-regulatory applicant code and/or rules, other measures)*	Note that there is a reference error in requirement 39 as the question asks what measures does the applicant take to ensure compliance with the APEC Information Privacy Principles. The principles in reference in requirement 39 refer to the principles listed in the CBPR program requirements as noted in the assessment purpose of the accountability section. Although these principles correspond with the APEC Information Privacy Principles, the CBPR do not include the principle of preventing harm. APEC will likely fix this in a

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

detail. Also, organizations must keep records concerning their implementation of their Privacy Shield obligations.				subsequent update to the Program Requirements.
	6	**Lawfulness of processing**		
EU-U.S. Privacy Shield Principle 2. Choice • *An organization must offer individuals the opportunity to choose (opt-out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available*	6(1)(a)	*Consent*	**CBPR Program Requirements; Assessment Criteria 9(a), 13(a), 14, 15 & 16** • *Use of data for unrelated purposes requires express consent or must be compelled by law. Disclosure of data to other controllers for purposes unrelated to the original purpose, or transfer of data to processors for purposes other than the original purpose, requires express consent, or must be necessary to provide a requested service or product, or must be compelled by law.*	The aggregate effect of the CBPR "Use" and "Choice" Assessment Purposes and Assessment Criteria is that data can be used without choice or consent if the data is used for the purpose for which it was collected and/or related/compatible uses. The fundamental criterion in determining whether a purpose is compatible with or related to the states purposes is whether the extended usage stems from or is in furtherance of such purposes.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

mechanisms to exercise choice.			• *Applicants must ensure individuals are provided with a mechanism to exercise choice in cases where choice would be appropriate. A choice mechanism is not required where the consent would be implied or where an applicable qualification (exception) is identified – this includes "obviousness" or circumstances whereby consent can be inferred from the provision of information by the individual. It also includes all uses related to the original purpose based on the "use" assessment criteria above.*	
EU-U.S. Privacy Shield Principle 2. Choice • *Under the EU-U.S. privacy shield, a consumer has the ability to exercise a choice where the*	6(1)(b)	*Contractual Necessity*	**Intake Questionnaire; Choice & CBPR Program Requirements; Assessment Criteria 13(b)** • *Applicants do not need to provide a mechanism for choice where consent can*	The Choice section of the Intake Questionnaire seems to indicate that choice can be inferred where an individual provides information in connection with a product or service they requested – this may

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

information is to be disclosed to third parties or to be used for materially different purposes. It can be implied that where information is provided by a consumer to engage in a transaction, the organization can process that data without consent (i.e. similar to the basis of contractual necessity under the GDPR).			*be inferred from the provision of the individual's information (see (i) "Obviousness" under Qualifications to the Provision of Choice Mechanisms in the intake questionnaire).* • *Applicants can further process data for purposes incompatible with the original where necessary to provide a service or product requested by the individual.*	well be in the context of a transaction or to enter into a contract and is similar to the contractual necessity ground for processing under the UK Regulation.
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is necessary for the establishment of*	6(1)(c)	Compliance with a legal obligation	**Intake Questionnaire; Choice & CBPR Program Requirements; Assessment Criteria 9(b) and 13** • *Applicants do not need to provide a mechanism for choice where disclosure is made (1) to law enforcement agencies for certain investigation purposes; (2) to third parties pursuant to a*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

legal claims or defenses. **EU-U.S. Privacy Shield Supplemental Principles 16. Access Requests by Public Authorities** • *Absence of notice in accordance with point (a)(xii) of the Notice Principle shall not prevent or impair an organization's ability to respond to any lawful request.*			*lawful form of process (e.g. discovery requests); (3) for purposes relating to investigations regarding violations of codes of conduct, breaches of contract or contravention of domestic law (see (v), (vi) and (vii) under Qualifications to the Provision of Choice Mechanisms in the intake questionnaire).* • *Applicants do not need to provide a mechanism for choice for further processing unrelated to the original purpose where such processing is compelled by applicable laws.* • *Applicants do not need to provide a mechanism for choice to disclose personal information to third party controllers or processors for further processing*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			unrelated to the original purposes where such disclosure is compelled by applicable laws.	
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is in the vital interests of the data subject or another person.*	6(1)(d)	*Protection of vital interests*	**Intake Questionnaire; Choice** • *Applicant does not need to provide a mechanism for choice in emergency situations that threaten the life, health or security of an individual.*	
No equivalent in EU-U.S. Privacy Shield	6(1)(e)	*Public interest*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	6(1)(f)	*Legitimate Interest*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *An organization may not process personal*	6(4)	*Compatible Purposes*	**CBPR Program Requirements; Assessment Criteria 8 & 12** • *Applicant must only use or disclose personal information it collects to*	Under the CBPR, applicants can process data for further incompatible purposes if such processing is based on express consent or if compelled by applicable

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. • *Depending on the circumstances, examples of compatible processing purposes may include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection.*			*fulfill the original purpose of collection or another compatible or related purpose.*	laws (See CBPR Program Requirements' Assessment Criteria 9 and 13). Under the GDPR, if the processing is deemed incompatible after taking into account the factors listed in Article 6(4) GDPR, then a new legal basis to conduct the processing may be required. This could include consent or necessity for compliance with a legal obligation.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

	7	**Conditions of consent**		
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must retain their records on the implementation of their Privacy Shield privacy practices (see Supplemental Principle 7(e)).* • *Organizations must have in place internal procedures for periodically conducting objective reviews of compliance. This impliedly includes records of consumer choices where choice is made on an opt-in basis (e.g. in the context of sensitive data processing).*	7(1)	*Demonstrable* • *Controller must be able to demonstrate that the data subject has consented to processing.*	**No Direct Equivalent in CBPR**	Indirectly implied via CBPR Program Requirements; Assessment Criteria 20. • Applicant must have policies or procedures in place specifying how preferences expressed through choice mechanisms are honored in an effective and expeditious manner. Having a choice mechanism in place and enabling preferences to be honored implies that such consent would be recorded and demonstrable by the applicant.
EU-U.S. Privacy Shield Principle 2. Choice	7(2)	*Distinguishable*	**CBPR Program Requirements; Assessment Criteria 17, 18 and 19**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.*		• *Controller must present the request for consent in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.*	• *Applicant's choice mechanism must be (1) displayed in a clear and conspicuous manner; (2) clearly worded and easily understandable; and (3) easily accessible and affordable.*	
No equivalent in EU-U.S. Privacy Shield	7(3)	*Withdrawal of consent*	**CBPR Program Requirements; Assessment Criteria 9(a), 13(a), 14, 15 & 16** • *In cases where obtaining express consent is required under the CBPR (i.e. for uses of data for unrelated purposes or disclosures of data to other controllers or transfers of data to processors for purposes other than the original purpose), the choice mechanisms facilitating such consent should provide an opportunity for individuals to withdraw consent. For example, via preference/profile pages;*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			email as well as other means.	
No equivalent in EU-U.S. Privacy Shield	7(4)	*Services conditional on consent to processing of personal data*	**No Equivalent in CBPR**	
	8	**Conditions applicable to child's consent in relation to information society services**		
No equivalent in EU-U.S. Privacy Shield	8(1)	*Age of consent* • *In relation to the offer of information society services, where a child is under the age of 13, processing is only lawful where consent is given or authorised by the holder of parental responsibility over the child.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	8(2)	*Parental consent verification* • *The controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child.*	**No Equivalent in CBPR**	
	9	**Processing special categories of personal data**		
EU-U.S. Privacy Shield Principle 2. Choice	9(1)	*Special categories of data*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *For sensitive information, organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice.* • *Sensitive information is considered personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or*		• *Processing of data regarding race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life or sexual orientation shall be prohibited unless an exception applies.*		

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

information specifying the sex life of the individual • *Organizations should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.*				
EU-U.S. Privacy Shield Principle 2. Choice • *For sensitive information, organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the*	9(2)(a)	*Explicit consent*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

individuals through the exercise of opt-in choice.				
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is necessary to carry out the organization's obligations in the field of employment law.*	9(2)(b)	*Obligation under employment and social security and social protection law*	**Intake Questionnaire; Choice & CBPR Program Requirements; Assessment Criteria 9(b) and 13** • *Applicants do not need to provide a mechanism for choice where disclosure is made to third parties pursuant to a lawful form of process.* • *Applicants do not need to provide a mechanism for choice for further processing unrelated to the original purpose where such processing is compelled by applicable laws.* • *Applicants do not need to provide a mechanism for choice to disclose personal information to third party*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			controllers or processors for further processing unrelated to the original purposes where such disclosure is compelled by applicable laws.	
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is in the vital interests of the data subject or another person.*	9(2)(c)	*Vital interests*	**Intake Questionnaire; Choice** • *Applicant does not need to provide a mechanism for choice in emergency situations that threaten the life, health or security of an individual.*	
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with*	9(2)(d)	*Legitimate activities by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim*	**No Equivalent in CBPR**	Note that it is unlikely that CBPR certified entities will be confronted with such processing scenarios as foundations, associations and other not-for-profit body with a political, philosophical, religious or

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

respect to sensitive data where the processing is carried out in the course of legitimate activities by a foundation, association or any other non-profit 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 the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.				trade union aim cannot certify under the CBPR system. As a result of the point above, for purposes of this mapping exercise, we are counting this provision as not relevant. To the extent that certifying organization engages in such activities, it can process sensitive data where the activity comprises the primary purpose of processing or a related purpose. If the activity constitutes processing that is unrelated to the original purpose, then the **CBPR is more privacy protective than the GDPR in this context as choice must always be given for such processing** (unless an appropriate qualification to choice applies).

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is related to data that are manifestly made public by the individual.*	9(2)(e)	*Data publicly disclosed by data subject*	**No Equivalent in CBPR**	Publicly available information is not covered by the CBPR (see Qualifications to the Provision of Notice and Choice Mechanisms in the intake questionnaire).
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is necessary for the establishment of*	9(2)(f)	*Establishment, exercise or defense of legal claims*	**Intake Questionnaire; Choice** • *Applicants do not need to provide a mechanism for choice where disclosure is made (1) to law enforcement agencies for certain investigation purposes; (2) to third parties pursuant to a lawful form of process (e.g. discovery requests); (3) for purposes relating to investigations regarding violations of codes of*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

legal claims or defenses.			*conduct, breaches of contract or contravention of domestic law (see (v), (vi) and (vii) under Qualifications to the Provision of Choice Mechanisms in the intake questionnaire).*	
No equivalent in EU-U.S. Privacy Shield	9(2)(g)	*Reasons of substantial public interest*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for reasons of substantial public interest under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				appropriate qualification applies.
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is required to provide medical care or diagnosis.*	9(2)(h)	*Purposes of preventive or occupational medicine*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for purposes of preventive or occupational medicine under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an appropriate qualification applies.
No equivalent in EU-U.S. Privacy Shield	9(2)(i)	*Public health*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				reasons of public interest in the area of public health, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an appropriate qualification applies.
No direct equivalent in EU.U.S. Privacy Shield; however, Privacy Shield Supplemental Principles 14. Pharmaceutical and Medical Products provides that: • *Where personal data collected for one research study are*	9(2)(j)	*Research or statistical purposes*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for research or statistical purposes under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is unrelated to

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

transferred to a U.S. organization in the Privacy Shield, the organization may use the data for a new scientific research activity if appropriate notice and choice have been provided in the first instance. Such notice should provide information about any future specific uses of the data, such as periodic follow-up, related studies, or marketing. • *It is understood that not all future uses of the data can be specified, since a new research use could arise from new insights on the original data, new medical discoveries and advances, and public health and regulatory developments. Where*				the original purpose. Where such processing is unrelated to the original purpose, the CBPR is more privacy protective than the GDPR in this context as express consent must always be given for such unrelated processing unless an appropriate qualification applies.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

appropriate, the notice should therefore include an explanation that personal data may be used in future medical and pharmaceutical research activities that are unanticipated. If the use is not consistent with the general research purpose(s) for which the personal data were originally collected, or to which the individual has consented subsequently, new consent must be obtained.				
EU-U.S. Privacy Shield Supplemental Principles 1. Sensitive Data • *An organization is not required to obtain affirmative express consent (opt in) with*	9(3)	*Processing for purposes of preventive or occupational medicine by or under the responsibility of a professional subject to the obligation of professional secrecy*	**No Equivalent in CBPR**	Although there is no specific provision permitting the processing of sensitive data for purposes of preventive or occupational medicine by or under the responsibility of a professional subject to

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

respect to sensitive data where the processing is required to provide medical care or diagnosis.				the obligation of professional secrecy under the CBPR, processing of sensitive data for such purposes can take place without express consent unless such processing is for a purpose unrelated to the original purpose. In such cases, **the CBPR is more privacy protective than the GDPR in this context as choice must always be given for such unrelated processing** unless an appropriate qualification applies.
No equivalent in EU-U.S. Privacy Shield	10	**Processing of personal data relating to criminal convictions and offences**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	11	**Processing which does not require identification** • *Controller shall not be obliged to process or acquire further information to identify a data subject for the sole purpose of complying with the regulation.*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as CBPR requirements only relate to personal information (i.e. information that is personally identifiable).

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		• *The rights under Articles 15 to 20 of the GDPR shall not apply except where the data subject provides additional information enabling his or her identification for the purpose of exercising such rights.*		
	12	**Transparent information, communication and modalities for the exercise of the rights of the data subject**		
EU-U.S. Privacy Shield Principle 1. Notice • *An organization must inform individuals of the information listed in (a)(i)-(xiii), which includes information about the right of individuals to access their personal data and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data.*	12(1)	*Transparent information and form* • *The controller shall provide information, communications and the modalities for the exercise of rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language.*	**CBPR Program Requirements; Assessment Criteria 1 and 38(a)** • *Applicant must provide clear and easily accessible statements about its practices and policies that govern the personal information* • *Applicant must provide access and correction mechanisms in a clear and conspicuous manner.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable.*				
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*	12(2)	*Facilitating data subject rights* • *The controller shall facilitate the exercise of rights and not refuse to act on a request to exercise such rights unless it is not in a position to identify the data subject.*	**CBPR Program Requirements; Assessment Criteria 22, 36 and 37** • *Applicant must have mechanisms in place to enable individuals to access or correct their personal information.* • *Applicant must grant access to any individual to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity.*	Note that the CBPR does not include inability to verify the identity of an individual as a qualification to the provision of access and correction. The qualifications listed in the CBPR include where providing access or correction would result in a disproportionate burden on the personal information controller, where information cannot be disclosed due to legal or security reasons or to protect confidential commercial information or where provision of access

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Consistent with the fundamental nature of access, organizations should always make good faith efforts to provide access.* • *Organizations must make good faith efforts to provide individuals with access to their personal data, the circumstances in which organizations may restrict such access are limited, and any reasons for restricting access must be specific.* • *An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity*				or correction would infringe the privacy rights of other persons.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

of the person making the request.				
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.* **EU-U.S. Privacy Shield Supplemental Principle 8. Access** • *Organizations should respond to access requests within a reasonable time period, in a reasonable manner, and in a form*	12(3)	*Responding to exercise of rights* • *The controller shall provide information on action taken on a request to exercise rights to the data subject without undue delay and in electronic form if the request was made by such means.*	**CBPR Program Requirements; Assessment Criteria 36, 37(b), (d) and 38(d)** *Form* • *In responding to an access request, applicant must provide information in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc.)* *Information on Action Taken* • *In responding to an access request, the applicant must provide confirmation of whether or not it holds personal information about the requester (unless an applicable qualification applies)* • *In responding to a request to exercise correction*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

that is readily intelligible to the individual.			*rights, applicant must provide a copy of the corrected personal information to the individual or confirmation that the data has been corrected or deleted.* *Timing* • *Applicant must provide access within a reasonable timeframe following an individual's request to access their data.*	
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *If an organization determines that access should be restricted in any particular instance, it should provide the individual requesting access with an explanation of why it has made that determination and a*	12(4)	*Controller not taking action* • *If the controller does not take action on a request to exercise rights, it shall inform the data subject without delay.*	**CBPR Program Requirements; Assessment Criteria 38(e)** • *If access or correction is refused, applicant must provide the individual with an explanation of why access or correction will not be provided, together with the contact information for further inquiries about the denial of access or correction.*	The CBPR provides the following qualifications to the provision of access and correction: (1) where providing access or correction would result in a disproportionate burden on the personal information controller, (2) where information cannot be disclosed due to legal or security reasons or to protect confidential commercial information or (3) where provision of

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

contact point for any further inquiries. • *An organization which claims an exception has the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.*				access or correction would infringe the privacy rights of other persons.
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *An organization may charge a fee that is not excessive.* • *Charging a fee may be justified (e.g., where requests for access are manifestly excessive, in particular because of their repetitive character).*	12(5)	*Applicable fees* • *Information and communication and actions regarding requests to exercise rights shall be provided free of charge unless where requests are manifestly unfounded or excessive.*	**Intake Questionnaire; Access and Correction & CBPR Program Requirements; Assessment Criteria 37(e)** • *Applicant does not need to provide access and correction where the expense of doing so would be unreasonable (e.g. where claims for access are repetitious or vexatious).*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Access may not be refused on cost grounds if the individual offers to pay the costs.*			• *If applicant charges a fee for providing individuals access to their data, it must describe the basis for the fee and how it ensures the fee is not excessive.*	
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *An organization is not required to provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.*	12(6)	*Identification of requestor* • *The controller may request additional information necessary to confirm the identity of the data subject.*	**CBPR Program Requirements; Assessment Criteria 36 and 37(a)** • *Applicant must grant access to any individual to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. Applicant must take steps to confirm the identity of the individual requesting access.*	
No equivalent in EU-U.S. Privacy Shield	12(7)	*Icons* • *Information to be provided under the Regulation may be provided in combination with standardized icons.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

	13	**Information to be provided where personal data are collected from the data subject**		
EU-U.S. Privacy Shield Principle 1. Notice • *An organization must inform individuals of the information listed in (a)(i)-(xiii), which includes, e.g., the types of personal data collected; the purposes for which the organization collects and uses personal information; how an individual can contact the organization with any inquiries or complaints; the type of third parties to which the organization discloses personal information, and the purposes for which it does so; the right of individuals to access*	13(1)	*Information to be provided* • *The controller must provide at the time when personal data are obtained the information listed in Article 13(1) at the time of collection to the data subject, where personal data is collected directly from the data subject. These include the identity and contact details of the controller and DPO, the purpose and legal basis for processing, the recipients of the personal data, the categories of data concerned, the intention to transfer data to a third country or international organization, the legal basis for the intended international transfer and the legitimate interests of the controller if the processing is conducted on that basis.*	**CBPR Program Requirements; Assessment Criteria 1(a)-(f), 2, 3 and 4** • *Applicant must provide statements about its practices and policies that govern personal information, including how personal information is collected (including types of data, and whether data is collected directly or through a third party or agent and the categories or specific sources of collected data), the purpose of collection, whether personal information is made available to third parties and for what purposes, the name of the applicant's company and location, including contact*	Note that unlike the GDPR, the CBPR does not include the concept of legitimate interest and as a result does not contain a transparency requirement for the use of such a basis to process data.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

their personal data; and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data. • *This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information, or as soon thereafter as is practicable.*			*information, information about the use and disclosure of an individual's personal information and how an individual can access and correct their data.* • *Applicant must provide at the time of collection of personal information (whether directly or through the use of third parties acting on its behalf) notice that information is being collected.*	
EU-U.S. Privacy Shield Principle 1. Notice • *Either when first collecting the personal information or as soon thereafter as practicable, an organization must inform individuals of the information listed in (a)(i)-(xiii), which*	13(2)	*Further information for fair and transparent processing* • *The controller must provide at the time when personal data are obtained further information enumerated in Article 13(2) to the data subject to ensure fair and transparent processing. These include the period for which the data will be stored or*	**CBPR Program Requirements; Assessment Criteria 1(f), 2** • *Applicant must provide information regarding whether and how and individual can access and correct their personal data.* • *Applicant must provide at the time of collection of*	Note that while the CBPR includes a requirement mandating certain further information to be provided to the data subject on top of those enumerated in Article 13(1), the CBPR only requires information about the existence of the right to request access to and rectification of personal data when compared

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

includes, e.g., how an individual can contact the organization with any inquiries or complaints; the right of individuals to access their personal data; and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data.		*criteria to determine the storage period, the existence of the right to request access, correction, erasure, restriction or objection to the processing data, as well as portability, the existence of the right to withdraw consent and lodge a complaint with the Commissioner, whether the provision of personal data is a statutory or contractual requirement or necessary to enter into a contract and meaningful information about the logic involved in some types of automate decision-making.*	*personal information (whether directly or through the use of third parties acting on its behalf) notice that information is being collected.*	against the requirements of Article 13(2) GDPR (e.g. there is no requirement to provide information about the right to lodge a complaint to the Commissioner, provide information about the existence of automated decision-making, other rights such as data portability etc.)
EU-U.S. Privacy Shield Principle 1. Notice • *Notice must be provided before the organization uses the information for a purpose other than that for which it was originally collected or processed by the*	13(3)	*Further processing* • *Prior to further processing of data for purposes other than that which the data was collected, the controller must provide to the data subject information about that further purpose of processing.*	**CBPR Program Requirements; Assessment Criteria 9 and 13** • *Applicant may further use, disclose or transfer personal information it collects for purposes other than which the data was collected if it bases such further processing on consent or in order to fulfill*	Note that if further processing data on the basis of separate consent or to provide a service or product requested by the individual, the applicant will need to communicate such further processing purposes to individuals when seeking consent or in the context of

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

transferring organization or discloses it for the first time to a third party.			*a legal obligation. In the case of disclosure or transfer, further processing is permitted to provide a service or product requested by the individual.*	the transaction to provide products or services.
EU-U.S. Privacy Shield Supplemental Principle 15. Public Record and Publicly Available Information • *It is not necessary for an organization to apply the Notice, Choice, or Accountability for Onward Transfer Principles to public record information, as long as it is not combined with non-public record information, and any conditions for consultation established by the*	13(4)	*Exception* • *The information requirements of Article 13 do not apply if the data subject already has the information.*	**No Equivalent in CBPR**	Note that while this specific exception to the requirement to provide notice does not appear in the CBPR, if an individual already has the information then the CBPR notice requirements may not apply as a matter of practice (see (i) "Obviousness" under Qualifications to the Provision of Notice in the intake questionnaire).

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

relevant jurisdiction are respected. • *It is generally not necessary for an organization to apply the Notice, Choice, or Accountability for Onward Transfer Principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those Principles by the organization for the uses it intends.*				
	14	**Information to be provided where personal data have not been obtained from the data subject**		
EU-U.S. Privacy Shield Principle 1. Notice • *The Privacy Shield notice principle appears*	14(1)	*Information to be provided* • *The controller must provide the information listed in Article 14(1) to the data*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 1(a)-(f), 2, 3 and 4**	The CBPR limits the provision of notice to the individual where personal data has not been obtained from the data subject to

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

to apply regardless of whether information is collected directly or through a third party. • *See Privacy Shield criteria corresponding to Article 13(1) GDPR above.*		*subject, where personal data has not been obtained from the data subject. These include the identity and contact details of the controller and DPO, the purposes of the processing and legal basis, the categories of personal data, the recipients, intention to transfer personal data to a third country or international organizations and the basis for transfer.*	• *Under the CBPR notice requirements, the applicant must identify in the privacy statement whether personal information is made available to third parties and for what purpose.* • *Disclosure of data to other controllers for purposes unrelated to the original purpose requires express consent, or must be necessary to provide a requested service or product, or must be compelled by law. For cases, where express consent is required, the individual will be notified of the new purpose of processing.* • *However, the recipient of the data is not obligated to provide notice to the individuals at or before the time of the collection (see*	notice stemming from the applicant that shared the data rather than from the recipient (as envisaged under Article 14(1) of the GDPR). This may be in the form of notice provided at the initial point of collection which specifies with whom the data may be shared and for what purpose or when the information is shared for unrelated purposes and express consent is sought from the individual.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			Qualifications to the Provision of Notice in the Intake Questionnaire).	
EU-U.S. Privacy Shield Principle 1. Notice • *An organization must inform individuals of the information listed in (a)(i)-(xiii), which includes, e.g., how an individual can contact the organization with any inquiries or complaints; the right of individuals to access their personal data; and the choices and means the organization offers individuals for limiting the use and disclosure of their personal data.*	14(2)	*Further information for fair and transparent processing* • *The controller must provide further information enumerated in Article 14(2) to the data subject to ensure fair and transparent processing. These include the period for which the data will be stored or criteria to determine the storage period, the fact that processing is based on legitimate interests, the existence of the right to request access, correction, erasure, restriction of, or objection to, the processing data, as well as portability, the existence of the right to withdraw consent and to lodge a complaint with the Commissioner, the source of the data and meaningful information about the logic*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 1(a) and (f)** • *Applicant must report the specific sources of all categories of personal information collected.* • *Applicant must provide information regarding whether and how and individual can access and correct their personal data.*	The CBPR limits the provision of notice to the individual where personal data has not been obtained from the data subject to notice stemming from the applicant that shared the data rather than from the recipient. Note that while the CBPR includes a requirement mandating certain further information to be provided to the data subject on top of those enumerated in Article 14(1), the CBPR only requires information about the existence of the right to request access to and rectification of personal data as well as the source from which the personal data originate when compared against the requirements of Article

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		involved in some types of automate decision-making.		14(2) GDPR (e.g. there is no requirement to provide information about the right to lodge a complaint, provide information about the existence of automated decision-making, other rights such as data portability etc.)
EU-U.S. Privacy Shield Principle 1. Notice • *Notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable.* • *Notice must be provided before the organization uses such information for a purpose other than that for which it was originally collected or*	14(3)	*Timing for provision of information* • *The controller must provide the information enumerated in Articles 14(1) and (2) within either a reasonable period after obtaining the data, at the time of first communication with the data subject (if the data is obtained for such purposes) or at the time the personal data are first disclosed to another recipient.*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 2, 3 and 4** • *Applicant must provide at the time of collection of personal information notice that information is being collected.* • *Applicant must explain to individuals the purposes for which information is being collected and that their personal information will be or may be shared with third parties and for what purposes.*	Although there is a timing requirement for the provision of notice in the CBPR, the CBPR limits the provision of notice to the individual where personal data has not been obtained from the data subject to notice stemming from the applicant that shared the data rather than from the recipient.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

processed by the transferring organization or discloses it for the first time to a third party.				
EU-U.S. Privacy Shield Principle 1. Notice • *Notice must be provided before the organization uses personal information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.*	14(4)	*Further processing* • *Prior to further processing of data for purposes other than that which the data was obtained, the controller must provide to the data subject information about that further purpose of processing.*	**No Equivalent in CBPR but consider CBPR Program Requirements; Assessment Criteria 9 and 13** *Applicant may further use, personal information it collects (including indirectly) for purposes other than which the data was collected if it bases such further processing on express consent or in order to fulfill a legal obligation.* *In the case of disclosure to third parties or transfers to processors, further processing is permitted on the basis of express consent, to provide a service or product requested by the individual or to fulfil a legal obligation.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			In cases of express consent or to provide a service or product requested by an individual, applicant will need to provide notice about the further purposes of processing.	
EU-U.S. Privacy Shield Supplementary Principle 4. Performing Due Diligence and Conducting Audits • *The activities of auditors and investment bankers may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles in certain circumstances (see below).* • *Investment bankers and attorneys engaged in due diligence, or auditors conducting an*	14(5)	*Exceptions* • *The information requirements of Article 14 do not apply if the data subject already has the information, the provision of such information proves impossible or would involve a disproportionate effort, or provision of the information would render impossible or seriously impair the achievement of the objectives of processing, obtaining or disclosing the information is expressly laid down in domestic law or the data is subject to an obligation of professional secrecy.*	**No Equivalent in CBPR but consider Intake Questionnaire; Notice** • *Applicants do not need to provide notice do not need to provide notice under certain circumstances (see (v) under Qualifications to the Provision of Notice in the intake questionnaire) – disclosure to a third party pursuant to a lawful form of process.*	Note that the exception to providing notice where collection of information is laid down in law maps to the CBPR qualification to notice of disclosure to a third party pursuant to a lawful form of process. However, the other exceptions laid down in Article 14(5) GDPR do not seem to have a direct equivalent in the CBPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

investment bankers or auditors.				
	15	**Right of access by the data subject**		
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.* **EU-U.S. Privacy Shield Supplemental Principle 8. Access** • *Individuals must have access to personal information about them that an organization*	15(1)	*Scope* • *The data subject has the right to obtain confirmation of and information about the data processing and a copy of his or her data from the controller.*	**CBPR Program Requirements; Assessment Criteria 36** • *Applicant must provide confirmation of whether it holds personal information about a requesting individual and must grant access (unless it identifies an applicable qualification) to personal information collected or gathered about that individual upon confirming the individual's identity.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

holds, including the purposes of the processing, the categories of personal information concerned, and the recipients or categories of recipients to whom the personal information is disclosed.				
No equivalent in EU-U.S. Privacy Shield	15(2)	*Transfers to third countries or international organizations* • *The data subject also has the right to be informed of appropriate safeguards for the transfer of his or her data to a third country or international organization.*	**No Equivalent in CBPR**	**FFD**
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Access can be provided in the form of disclosure of the relevant personal information by an*	15(3)	*Fees and form of delivery* • *The controller shall provide a copy of personal data undergoing processing and may charge a reasonable fee for further requested copies. Where the access request is*	**CBPR Program Requirements; Assessment Criteria 37 (d) and (e)** *Fee* • *If applicant charges a fee for providing individuals access to their data, it*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

organization to the individual and does not require access by the individual to an organization's data base. • *Charging a fee may be justified (e.g., where requests for access are manifestly excessive, in particular because of their repetitive character).* • *Access may not be refused on cost grounds if the individual offers to pay the costs.*		*made by electronic means, the information shall also be provided by such means unless otherwise requested by the data subject.*	*must describe the basis for the fee and how it ensures the fee is not excessive.* *Form* • *In responding to an access request, applicant must provide information in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc.)*	
Privacy Shield Supplemental Principle 8. Access • The right of access to personal information may be restricted in exceptional circumstances where	15(4)	*Third party rights* • *The right to obtain a copy of the data shall not adversely affect the rights and freedoms of others.*	**Intake Questionnaire; Access and Correction** • *Personal information controllers do not need to provide access where the information privacy of persons other than the individual would be*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the legitimate rights of persons other than the individual would be violated. • The right of access to personal information may be restricted where the legitimate rights or important interests of others would be violated			*violated (though it must provide access where the third party's personal information can be severed from the information requested after such third party's information is redacted) (see Qualifications to the Provision of Access and Correction Mechanisms – (iii) Third Party Risk – in the intake questionnaire).*	
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*	16	**Right to rectification** • *The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data or the completion of incomplete personal data concerning him or her.*	**CBPR Program Requirements; Assessment Criteria 38 (b) and (c)** <u>*Right*</u> • *Applicant must make requested corrections or additions to personal information about an individual if that individual demonstrates the personal information held about them by the applicant is incomplete or incorrect.* <u>*Timing*</u>	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*			• *Applicant must make such corrections or additions within a reasonable timeframe following the request.*	
	17	**Right to erasure**		
EU-U.S. Privacy Shield Principle 6. Access • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate,*	17(1)	*Applicability and cases for erasure* • *Data subject has the right to obtain from the controller the erasure of personal data where the data is no longer necessary, the data subject has withdrawn consent to processing based on consent, the individual objects to the processing and there are no overriding legitimate grounds*	**CBPR Program Requirements; Assessment Criteria 38** • *Applicant must permit individuals to challenge the accuracy of their information and have it deleted, where appropriate (subject to applicable qualifications).*	The CBPR requirements for access and correction provide a limited overlap with the GDPR right to be forgotten. Under the CBPR, deletion requests can be made where data held by the personal information controller is inaccurate.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

or has been processed in violation of the Principles. **EU-U.S. Privacy Shield Supplemental Principle 8. Access** • *Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.*		*for processing, the data has been unlawfully processed, the data has to be erased by law or the data has been collected in relation to the offer of information society services directed to children.*		

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

No equivalent in EU-U.S. Privacy Shield	17(2)	*Informing other controllers* • *Where the controller has made the personal data public and is obliged to erase it, the controller shall take reasonable steps to inform controllers processing the personal data that the data subject has requested erasure of the data.*	**No Equivalent in CBPR**	In the context of a request to correct information (which may include deleting information under the CBPR), there is a requirement to communicate corrections to third parties which is a very limited match to the requirements of Article 17(2).
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *The right of access to personal information may be restricted in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the*	17(3)	*Exceptions* • *Exceptions to the right of the erasure include where the processing is necessary for exercising the right of freedom of expression and information, compliance with legal obligations, reasons of public interest in area of public health, archiving purposes in the public interest or scientific, historical research and statistical purposes, and the establishment, exercise or defense of legal claims.*	**Intake Questionnaire; Access and Correction** *Personal information controllers do not need to provide correction (and by extension deletion per Assessment Criteria 38 in the CBPR Program Requirements) where information cannot be disclosure due to legal or security reasons.*	Note that the exception contained in the CBPR could in theory be read broadly to cover several of the GDPR exceptions, including, compliance with legal obligations, for reasons of public interest in the area of public health or the establishment, exercise or defense of legal claims.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

individual's privacy in the case in question. • *Organizations may deny or limit access to the extent that granting full access would reveal its own confidential commercial information.* • *Organizations can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

purposes, access may be denied. • *Other reasons for denying or limiting access are:* o *interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;* o *disclosure where the legitimate rights or important interests of others would be violated;*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

o *breaching a legal or other professional privilege or obligation;* o *prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or* o *prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

management, or in future or ongoing negotiations involving the organization.				
No equivalent in EU-U.S. Privacy Shield	18	**Right to restriction of processing**	**No Equivalent in CBPR**	**FFD**
No equivalent in EU-U.S. Privacy Shield	19	**Notification obligation regarding rectification or erasure of personal data or restriction of processing** • *The controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the data have been disclosed unless this is impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if he or she requests it.*	**CBPR Program Requirements; Assessment Criteria 23, 24 and 46** • *Applicant must communicate corrections of personal information to personal information processors, agent, other service providers and other third parties to whom personal information was transferred/disclosed.* • *Applicant must also have mechanism in place with personal information processors, agents, contractors or other*	Note that correction in the CBPR includes deletion of data.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			service providers to ensure that the applicant's obligations to the individual will be met.	
No equivalent in EU-U.S. Privacy Shield	20	**Right to data portability**	**No Equivalent in CBPR**	
	21	**Right to object**		
• **No equivalent in EU-U.S. Privacy Shield**	21(1)	*Objection based on public interest and legitimate interests* • *The data subject shall have the right to object to processing based on public interest or legitimate interest, including profiling based on such provisions. The controller shall no longer process the data unless it demonstrates compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 12. Choice – Timing of Opt Out	21(2)	*Objection to direct marketing* • *The data subject shall have the right to object at any time*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Individuals should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization time to make the opt out effective.*		*to processing of his or her personal data for direct marketing purposes.*		
EU-U.S. Privacy Shield Supplemental Principle 12. Choice – Timing of Opt Out • *Individuals should be able to exercise "opt out" choice of having personal information used for direct marketing at any time subject to reasonable limits established by the organization, such as giving the organization*	21(3)	*Cessation of processing for direct marketing* • *Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

time to make the opt out effective.				
EU-U.S. Privacy Shield Principle 2. Choice: • *Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.* **EU-U.S. Privacy Shield Supplemental Principle 12. Choice – Timing of Opt Out** • *An organization may use information for certain direct marketing purposes when it is impracticable to provide the individual with an opportunity to opt out before using the information, if the organization promptly gives the individual such opportunity at the*	21(4)	*Transparency* • *At the latest at the time of first communication with the data subject, the right to object to processing based on public or legitimate interest or for direct marketing purposes shall be brought to the attention of the data subject.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

same time (and upon request at any time) to decline (at no cost to the individual) to receive any further direct marketing communications and the organization complies with the individual's wishes.				
EU-U.S. Privacy Shield Supplemental Principle 12. Choice - Timing of Opt Out • *Individuals may be able to exercise the opt out through the use of a central "opt out" program such as the Direct Marketing Association's Mail Preference Service. Organizations that participate in the Direct Marketing Association's Mail Preference Service should promote its availability to consumers who do not*	21(5)	*Technical specifications* • *In the context of the use of information society services, the data subject may exercise his or her right to object by automated means using technical specifications.*	**CBPR Program Requirements; Assessment Criteria 14, 15 and 16** • *Applicant must ensure individuals are provided with a mechanism for individuals to exercise choice in relation to the collection, use and disclosure of their personal information (unless an applicable qualification is identified and justified). These mechanisms include any appropriate means to exercise choice, including online at the point of the collection, via email, via*	While a right to object does not exist under the CBPR, the CBPR enables the exercise of choices through electronic and other means. **FFD**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

wish to receive commercial information. In any event, an individual should be given a readily available and affordable mechanism to exercise this option.			*preference/profile pages, via telephone, postal mail or other means.*	
No direct equivalent in EU-U.S. Privacy Shield. The Privacy Shield has a general opt-out provision, as listed above (Principle 2. Choice).	21(6)	*Objection to processing for research and statistical purposes* • *The data subject shall have the right to object to processing for scientific or historical research purposes or statistical purposes unless such processing is necessary for public interest reasons.*	**No Equivalent**	**FFD**
No equivalent in EU-U.S. Privacy Shield	22	**Automated individual decision-making, including profiling**	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 8. Access • *Organizations can restrict access to information to the*	23	**Restrictions** • *The Secretary of State may restrict the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as*	**Intake Questionnaire; Notice, Access and Correction** • *Applicant does not need to provide notice, access or correction under certain circumstances (see*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. In addition, where personal information is processed solely for research or statistical purposes, access may be denied. • *Other reasons for denying or limiting access are:* o *interference with the execution or enforcement of the law or with private causes of action, including the prevention,*		*Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22. When such restriction is necessary to safeguard: public security, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, other important objectives of general public interest, in particular an important economic or financial interest, the protection of judicial independence and judicial proceedings, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the monitoring, inspection or regulatory function connected to the exercise of official authority, the protection of the data subject or the rights and freedoms of others, the*	*Qualifications to the Provision of Notice in the Intake Questionnaire, namely – (iv) Disclosure to a government institution which has made a request for the information with lawful authority; (v) disclosure to a third party pursuant to a lawful form of process; (vii) for legitimate investigation purposes; (viii) action in the event of an emergency; see also the Qualifications to the Provision of Access and Correction in the Intake Questionnaire – (ii) protection of confidential information, including where information cannot be disclosed due to legal or security reasons; (iii) third party risk (i.e. where providing access would violate the information*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

investigation or detection of offenses or the right to a fair trial; o *disclosure where the legitimate rights or important interests of others would be violated;* o *breaching a legal or other professional privilege or obligation;* o *prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and*		*enforcement of civil law claims.*	*privacy of persons other than the requester).*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

corporate re-organizations; or o *prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving the organization.*				
	24	**Responsibility of the controller**		
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must provide follow up procedures for verifying that the attestations and assertions they*	24(1)	*Accountability* • *The controller must implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the Regulation and review and*	**CBPR Program Requirements; Assessment Criteria 39** *Applicant must have measures to ensure compliance with the CBPR program requirements (i.e. internal guidelines or policies, contracts, compliance with applicable industry or*	Note that there is a reference error in requirement 39 as the question asks what measures does the applicant take to ensure compliance with the APEC Information Privacy Principles. The principles in

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

make about their Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles. This can be done either through self-assessment or outside compliance reviews. Also, organizations must keep records concerning their implementation of their Privacy Shield obligations.		*update such measures where necessary.*	*sector laws and regulations, compliance with self-regulatory applicant code and/or rules, other measures)*	reference in requirement 39 refer to the principles listed in the CBPR program requirements as noted in the assessment purpose of the accountability section. Although these principles correspond with the APEC Information Privacy Principles, the CBPR do not include the principle of preventing harm. APEC will likely fix this in a subsequent update to the Program Requirements.
EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must provide follow up procedures for verifying that the attestations and assertions they make about their*	24(2)	*Policies* • *Where proportionate in relation to processing activities, the measures for compliance shall include the implementation of appropriate data protection policies by the controller.*	**CBPR Program Requirements; Assessment Criteria 39** • *Appropriate measures for ensuring compliance with the CBPR program requirements include the implementation of internal policies.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles.				
Not relevant to this mapping exercise as the EU-U.S. Privacy Shield is a certification.	24(3)	*Certification/Codes of conduct* • *Adherence to codes of conduct or approved certification mechanisms may be used to demonstrate compliance.*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as the CBPR is a certification.
	25	**Data protection by design and by default**		
EU-U.S. Privacy Shield Principles 4. Security, 5. Data Integrity and Purpose Limitation and Supplemental Principle 7. Verification • The principles of security, data integrity and purpose limitation and verification contemplate that the organization implement	25(1)	*Privacy by design* • *The controller shall implement appropriate technical and organizational measures which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing to meet the requirements of the*	**CBPR Program Requirements; Security Safeguards (Assessment Criteria 26-35) and Accountability (Assessment Criteria 39-50)**	The CBPR security safeguards and accountability provisions contemplate that the applicant shall implement appropriate technical and organizational measures to meet the CBPR program requirements and protect the rights of individuals.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

appropriate technical and organizational measures to meet the requirements of the EU-U.S. Privacy Shield Principles.		*Regulation and protect the rights of data subjects.*		
EU-U.S. Privacy Shield Supplemental Principle 5. Data Integrity and Purpose Limitation • *Organizations must limit personal information to that which is relevant for the purposes of processing and must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current.*	25(2)	*Privacy by default* • *The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Such measures must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*	**No Direct Equivalent in CBPR**	While the CBPR program requirements do not require technical and organizational measures that, by default, ensure only personal data which are necessary for processing are processed, assessment criteria 9 requires that the applicant limit the amount and type of personal information collected to that which is relevant to the stated purpose.
Not relevant to as the EU-U.S. Privacy Shield is a certification.	25(3)	*Certification/Codes of conduct* • *An approved certification mechanism may be used to demonstrate compliance with*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as the CBPR is a certification.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		the requirements of data protection by design and by default.		
No equivalent in EU-U.S. Privacy Shield	26	**Joint controllers**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	27	**Representatives of controllers or processors not established in the United Kingdom**	**No Equivalent in CBPR**	
	28	**Processor**		
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfers • *Where personal data is transferred to a third party acting as an agent, organizations must take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles.*	28(1)	*Processors providing sufficient guarantees* • *The controller must only use processors providing sufficient guarantees to implement appropriate technical and organizational measures to comply with the requirements of the Regulation and ensure protection of the rights of the data subject.*	**CBPR Program Requirements; Assessment Criteria 27, 46, 47, 48 and 49** • *Applicant must take reasonable measures to require information processors, agents, contractors or other services providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of information.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			• *Applicant must implement mechanisms with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicants obligations will be met (such mechanisms include internal guidelines or policies, contracts, compliance with applicable industry or sector laws and regulations, compliance with self-regulatory applicant code and/or rules, other measures).* • *Applicant must require processors to provide self-assessments to ensure compliance with the applicant's instructions and/or agreements or contracts.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			• *Applicant must carry out regular spot checking or monitoring of processors to ensure compliance with the applicant's instructions and/or agreements or contracts (or explain why it does not spot check or monitor).*	
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor understands whether onward transfer is allowed. This might include a requirement to obtain written authorization of the controller before engaging a subprocessor.*	28(2)	*Subprocessors* • *The processor shall not engage another processor without prior specific or general written authorisation of the controller.*	**CBPR Program Requirements; Assessment Criteria 47** • *Applicant must impose restrictions on subcontracting unless the applicant provides consent to the subcontracting arrangement.*	
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer	28(3)	*Data processing agreements* • *Processing by a processor shall be governed by a contract or*	**CBPR Program Requirements; Assessment Criteria 46 and 47**	Note that the specific contractual requirements for processor contracts set out in the CBPR are not

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Where personal information is transferred to an agent, the organization must provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.* **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *When personal data is transferred from the EU to the U.S. only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.*		*other legal act under domestic law that sets out the subject matter and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.*	• *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicants obligations will be met.*	identical to those enumerated in Article 28(3) GDPR but the principle of having a contract in place exists within the CBPR. See the following columns for more information about each specific contractual requirement required by Article 28(3) GDPR and how they map to the CBPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Data controllers in the EU are always required to enter into a contract when a transfer for processing is made, and whether or not the processor participates in the Privacy Shield.*				
Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The purpose of the contract is to make sure that the processor acts only on instructions from the controller.*	28(3)(a)	*Controller instructions* • *Processor must process the personal data only on documented instructions from the controller unless required by domestic law.*	**CBPR Program Requirements; Assessment Criteria 47** • *Processor must follow instructions provided by the applicant relating to the manner in which its personal information must be handled.*	
Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers *The purpose of the contract is to make sure that the processor acts only on*	28(3)(b)	*Commitment to confidentiality* • *Processor must ensure that persons authorized to process the data have committed themselves to confidentiality or are under a statutory obligation of confidentiality.*	**CBPR Program Requirements; Assessment Criteria 47** *Processor must follow instructions provided by the applicant relating to the manner in which its personal information must be handled.*	Any confidentiality obligations that are included in processor contracts will attach to persons authorized to process data by the processor entity.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

instructions from the controller. Any confidentiality obligations that are included in processor contracts will attach to persons authorized to process data by the processor entity.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and*	28(3)(c)	*Security* • *Processor must take all applicable security measures pursuant to Article 32 GDPR.*	**CBPR Program Requirements; Assessment Criteria 35(a)** • *Applicant must require processors to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of information by implementing an information security program.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles. **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *The contract should make sure that the processor provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access, and*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

understands whether onward transfer is allowed.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent*	28(3)(d)	*Conditions for subprocessing* • *Processor must respect the conditions for engaging another processor.*	**CBPR Program Requirements; Assessment Criteria 47** • *Applicant must impose restrictions on subcontracting unless it provides consent to the subcontracting arrangement.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor understands whether onward transfer is allowed.*				
EU-U.S. Privacy Shield Supplemental Principle 9. Human Resources Data • *With respect to the application of the Access Principle, the Privacy Shield requires that an organization processing data in the U.S. will cooperate in providing such access either directly or through the EU employer.* **EU-U.S. Privacy Shield Supplemental Principle 10.**	28(3)(e)	*Providing assistance to controller (data subject rights)* • *Processor must assist the controller in fulfilling its obligation to respond to requests for the exercise of rights.*	**CBPR Program Requirements; Assessment Criteria 23, 24 and 25** • *Processors must update inaccurate, incomplete or out of date information when notified by the Applicant following a request to correct personal information. Similarly, processors must notify the applicant when they become aware of information that is inaccurate, incomplete or out of date.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.*				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide*	28(3)(f)	*Providing assistance to controller (risk, security and breach notification)* • *Processor must assist the controller in ensuring compliance with the GDPR's requirements on security, breach notification and communication of breaches, data protection impact assessments and prior consultation for high risk processing.*	**CBPR Program Requirements; Assessment Criteria 35** • *Applicant must require processors to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of information by implementing an information security program, notifying the applicant promptly when*	Note that the CBPR does not include requirements around data protection impact assessments and, as a result, Assessment Criteria 35 does not map to this prong of Article 28(3)(f) GDPR. The Harms Principle in the APEC Information Privacy Principles articles a risk-based approach to all privacy measures, but that was not made explicit or included in the CBPR program requirements.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the same level of protection as is required by the Principles; and (ii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing.			*they become aware of a breach and taking steps to correct/address the security failure which caused the breach.*	
No equivalent in EU-U.S. Privacy Shield	28(3)(g)	*End of service requirements* • *Processor must delete or return all the personal data to the controller after the end of the provision of services and delete existing copies unless domestic law requires storage of the data.*	**No Equivalent in CBPR**	Note the APEC Privacy Recognition for Processors (PRP) system contains a provision regarding disposal of information by processors following the end of the provision of services. Also, while the CBPR does not explicitly require processors to delete or return all personal data at the end of provision of services, the agreement under Assessment Criteria 47 requires processors to abide by the Applicant's APEC-complaint privacy policies and practices and

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				Assessment Criteria 31 requires a policy for the secure disposal of information.
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; and (ii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's*	28(3)(h)	*Processor accountability* • *Processor must make available to the controller all information necessary to demonstrate compliance with the processor obligations laid down in Article 28 GDPR.*	**CBPR Program Requirements; Assessment Criteria 48 and 49** • *Applicant must require processors to provide self-assessments to ensure compliance with the applicant's instructions and/or agreements or contracts.* • *Applicant must carry out regular spot checking or monitoring of processors to ensure compliance with the applicant's instructions and/or agreements or contracts (or explain why it does not spot check or monitor).*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

obligations under the Principles.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent*	28(4)	*Subprocessor agreements* • *Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act.*	**No Direct Equivalent in CBPR**	Note that under the CBPR, if the applicant consents to the use of a sub-processor, which under the CBPR is a precondition to sub-processing, the applicant will likely require that sub-processor to adhere to the same requirements as the processor the applicant initially engaged.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with the organization's obligations under the Principles. **EU-U.S. Privacy Shield Principle 7. Recourse, Enforcement and Liability** • *In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

proves that it is not responsible for the event giving rise to the damage.				
No equivalent in EU-U.S. Privacy Shield	28(5)	*Certification/Codes of conduct* • *Adherence of a processor to an approved code of conduct or an approved certification may be used to demonstrate sufficient guarantees as referred to in Article 28 GDPR.*	**No Equivalent in CBPR**	Note that the APEC Privacy Recognition for Processors (PRP) system is available for this function.
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.*	28(6)	*SCCs* • *The contract or other legal act reference in Article 28 may be based, in whole or in part, on standard contractual clauses.*	**CBPR Program Requirements; Assessment Criteria 46** • *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicant's obligations will be met.*	While GDPR standard contractual clauses are irrelevant in the context of the CBPR, the CBPR permits the use of contracts to govern relationships with data processors.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

N/A	28(7)	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	28(8)	*Adoption of SCCs* • *The Commissioner may adopt standard contractual clauses for the matters referred to in Article 28.*	**No Equivalent in CBPR**	Not relevant to this mapping exercise.
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the Privacy Shield.* • *In practice, such contracts will most*	28(9)	*Form of contract/legal act* • *The contract or other legal act reference in Article 28 shall be in writing, including in electronic form.*	**CBPR Program Requirements; Assessment Criteria 46** • *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicant's obligations will be met.*	Under the CBPR, the applicant can implement mechanisms with processors to ensure their obligations can be met. The mechanism will almost always be a contract. The Accountability Agent must verify the existence of each type of agreement described (i.e. the contract) and this implies there will be at least a written contract. It is highly unlikely that such contracts would not also be available in electronic form.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

likely be in written and electronic form.				
No equivalent in EU-U.S. Privacy Shield. In contrast, Privacy Shield Principle 7. Recourse, Enforcement and Liability states: • *In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization*	28(10)	*Liability* • *If a processor infringes the Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.*	**No Equivalent in CBPR**	Under the CBPR, liability for infringements by processors is governed by contract and local laws in participating economies determine legal liability for any misconduct associated with relevant processing activities. The CBPR itself does not provide legal protection however for the scenario envisaged by Article 28(10) GDPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

proves that it is not responsible for the event giving rise to the damage. **EU-U.S. Privacy Shield Supplemental Principle 3. Secondary Liability** • *The Privacy Shield does not create secondary liability. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.* **EU-U.S. Privacy Shield Supplemental Principle 9. Human Resources Data – Enforcement**				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Where personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU.*				
EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *Where an organization engages a third party acting as an agent, the organization must implement a contract that should make sure the processor acts only on instructions from the controller.* • *Where an organization engages a third party*	29	**Processing under the authority of the controller or processor** • *The processor and any person acting under the authority of the controller or processor shall not process personal data except on instructions from the controller or if required to do so by domestic law.*	**CBPR Program Requirements; Assessment Criteria 12, 13, 46, 47, 48 and 49** • *If personal information is transferred to processors, such transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual or compelled by law.* • *Processors, agents, contractors or other*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

acting as a controller, the organization must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation.			*services providers must comply with the requirements of the applicant as set out under Assessment Criteria 46, 47, 48 and 49.*	
	30	**Records of processing activities**		

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 7. Verification • *Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the*	30(1)	*Types of records to be maintained by controller* • *Each controller and, where applicable, its representative, shall maintain a record of processing activities under its responsibility, including (a) name and contact details of controller, joint controller, representative and the DPO, (b) purposes of processing, (c) description of the categories of personal data and data subjects, (d) categories of recipients, (e) transfers of personal data to a third country/international organization, (f) envisaged time limits for erasure of categories of data, where possible and (g) a general description of the technical and organizational security measures under Article 32(1) GDPR or 28(3) of the UK Data Protection Act 2018, where possible.*	**CBPR Program Requirements; Assessment Criteria 6 & Assessment Purpose of "Integrity of Personal Information"** • *Accountability agent must require the Applicant to identify each type of data it collects, the corresponding state purpose of collection for each, all uses that apply to each type of data and an explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. By inference, the Applicant will need to retain records of such information.* • *The questions within the "Integrity of Personal Information" section of the CBPR are directed towards ensuring that the personal*	Note that while the CBPR program requirements impose a record keeping requirement, the specific types of information to be recorded are not identical to those enumerated under Article 30(1) GDPR.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Department relating to the organization's adherence to the Principles.			*information controller maintains the accuracy and completeness of records and keeps them up to date.*	
No equivalent in EU-U.S. Privacy Shield	30(2)	*Types of records to be maintained by the processor* • *Each processor and, where applicable, its representative shall maintain a record of processing activities carried out on behalf of the controller, containing (a) name and contact details of the processor and of the controller it acts on behalf of, (b) categories of processing carried out, (c) transfers of personal data to third country/international organization and (d) a general description of the technical and organizational security measures under Article 32(1) GDPR or 28(3) of the UK Data Protection Act 2018, where possible.*	**CBPR Program Requirements; Assessment Criteria 47 & Assessment Purpose of "Integrity of Personal Information"** • *Applicant must implement mechanisms, including contracts, with personal information processors, agents, contractors or other services providers pertaining to information they process on the applicant's behalf to ensure the applicants obligations will be met. Such an agreement must generally require such parties to implement privacy practices that are substantially similar to the applicant's policies or*	Under the CBPR, the applicant (i.e. controller) already has to maintain records and this obligation is passed on indirectly to processors as processors must implement privacy practices that are substantially similar to the applicant's policies or privacy practices by virtue of any contract entered into between the controller and processor.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			privacy practices (including the maintenance of complete and accurate records).	
No equivalent in EU-U.S. Privacy Shield	30(3)	*Form of records* • *Records of processing shall be in writing, including in electronic form.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 5. The Role of the Data Protection Authorities • *Organizations will implement their commitment to cooperate with EU supervisory authorities.* **EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer** • *Where an organization transfers personal data to a third party acting as an agent, the*	30(4)	*Making records available to Commissioner* • *Controller or processor shall make the record available to the Commissioner on request.*	**APEC CBPR Policies, Rules and Guidelines; CBPR Element 4 – Enforcement** • *Accountability Agents should be able to enforce the CBPR program requirements through law or contract.* • *The Privacy Enforcement Authorities should have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information*	Under the CBPR, certified organizations must participate in any dispute resolution requested by a consumer or the Accountability Agent and presumably provide records in the process. Moreover, certified organizations are subject to the jurisdiction of the Privacy Enforcement Authority in the jurisdiction in which they were certified and must respond to document requests from the Privacy Enforcement Authority in the context of an investigation.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

organization must provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request. **EU-U.S. Privacy Shield Supplemental Principle 7. Verification** • *Organizations must retain their records on the implementation of their Privacy Shield privacy practices and make them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for*			*consistent with the CBPR program requirements.* **Accountability Agent APEC Recognition Application; Recognition Criteria (Dispute Resolution Process and Mechanism for Enforcing Program Requirements)** • *An Accountability Agent must have a mechanism to receive and investigate complaints about Participants and to resolve disputes between complainants and Participants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents recognized by APEC economies when appropriate and where possible.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

investigating complaints or to the agency with unfair and deceptive practices jurisdiction. Organizations must also respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles. **EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement** • *Organizations, as well as their independent recourse mechanisms, must provide information relating to the Privacy Shield when*			• *Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC Cross-Border Privacy Rules System requirements has not been remedied within a reasonable time, so long as such failure to comply can be reasonably believed to be a violation of applicable law.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

requested by the Department.				
No equivalent in EU-U.S. Privacy Shield	30(5)	*Exceptions* • *The records of processing requirement shall not apply to an enterprise or organization employing fewer than 250 persons unless the processing is likely to result in a high risk to data subject, the processing is not occasional or the processing includes special categories of data.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplemental Principle 5. The Role of the Data Protection Authorities • *Organizations will implement their commitment to cooperate with EU supervisory authorities.* • *An organization commits to cooperate*	31	**Cooperation with the Commissioner**	**CBPR Program Requirements; Assessment Criteria 45** • *Organizations must have procedures in place for responding to judicial or other government subpoenas, warrants or orders.* **Accountability Agent APEC Recognition Application; Recognition Criteria**	The CBPR requires organizations to have procedures in place to respond to judicial or other government subpoenas, warrants or orders. In the context of cooperation with the Commissioner under Article 31 GDPR, the CBPR goes further with respect to responding to such requests by mandating specific procedures be put in place.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with EU supervisory authorities by declaring in its Privacy Shield self-certification submission to the Department of Commerce (see Supplemental Principle on Self-Certification) that the organization: ○ *elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with EU supervisory authorities;* ○ *will cooperate with EU supervisory authorities in*			• *Accountability Agents must have processes for ongoing monitoring, compliance reviews, annual recertification and dispute resolution in which certified organizations must participate and cooperate.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the investigation and resolution of complaints brought under the Privacy Shield; and ○ *will comply with any advice given by EU supervisory authorities where EU supervisory authorities take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, and will provide EU supervisory authorities with written*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

confirmation that such action has been taken. • *Organizations choosing the option for dispute resolution must undertake to comply with the advice of EU supervisory authorities.* • *An organization that wishes its Privacy Shield benefits to cover human resources data transferred from the EU in the context of the employment relationship must commit to cooperate with EU supervisory authorities with regard to such data (see Supplemental Principle on Human Resources Data).*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *The Privacy Shield provides for the establishment of DPA Panels will provide advice to the U.S. organizations concerned on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Privacy Shield. The panel will provide such advice in response to referrals from the organizations concerned and/or to complaints received directly from individuals against organizations which have committed to cooperate with EU supervisory authorities for Privacy Shield purposes, while*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

encouraging and if necessary, helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer. **EU-U.S. Privacy Shield Supplemental Principle 9. Human Resources Data – Enforcement** • *A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the EU in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must commit to cooperate in investigations by and to comply with the advice of competent EU*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

authorities in such cases. **EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement** • *Organizations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPAs.*				
	32	**Security of processing**		
EU-U.S. Privacy Shield Principle 4. Security • *Organizations creating, maintaining, using or disseminating personal information must take reasonable and appropriate measures to protect personal information from loss, misuse and*	32(1)	*Security measures* • *The controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including pseudonymization, the ability to ensure the ongoing CIA and resilience of processing systems and services, the*	**CBPR Program Requirements; Assessment Criteria 26, 27, 28, 30 (c) and (d), 32 and 33** • *Applicant must implement physical, technical and administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use,*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.		*ability to restore the availability and access to personal data in a timely manner in the event of an incident and a process for regularly testing, assessing and evaluating the effectiveness of measures for ensuring security of processing.*	*modification or disclosure of information or other misuses and such safeguards must be proportional to the likelihood and severity of harm threatened, the sensitivity of information and the context in which it is held.* • *Applicant must implement measures to detect, prevent and respond to attacks, intrusions or other security failures and have processes in place to test the effectiveness of these measures.* • *Applicant must implement physical security safeguards.*	
EU-U.S. Privacy Shield Principle 4. Security • *In taking reasonable and appropriate measures to protect*	32(2)	*Risk assessment* • *In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in*	**CBPR Program Requirements; Assessment Criteria 27, 28 and 34** • *Applicant must implement physical, technical and*	Certification in this context – language in the assessment criteria. We assume this means as a result of a review by a

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

personal information, organizations must take into due account the risks involved in the processing and the nature of the personal data.		*particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*	*administrative safeguards to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses and such safeguards must be proportional to the likelihood and severity of harm threatened, the sensitivity of information and the context in which it is held.* • *Applicant must adjust their security safeguards to reflect the results of certifications or risk assessments or audits.*	certification body/audit to adjust security.
Not relevant to this mapping exercise as the Privacy Shield is a certification.	32(3)	*Certification/Codes of conduct* • *Adherence to an approved code of conduct or certification mechanism may be used as an element by*	**No Equivalent in CBPR**	Not relevant to this mapping exercise as the CBPR is a certification.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		which to demonstrate security of processing.		
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles.*	32(4)	*Security instructions to agents of controller/processor* • *The controller or processor must take steps to ensure that any natural person acting under the authority of the controller or processor does not process data except on the instructions of the controller unless required to do so by law.*	**CBPR Program Requirements; Assessment Criteria 29 and 30(a)** • *Applicant must implement employee security training and management.*	
No equivalent in EU-U.S. Privacy Shield	33	**Notification of a personal data breach to the Commissioner**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	34	**Communication of a personal data breach to the data subject**	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	35	**Data protection impact assessment**	**No Equivalent in CBPR**	Note that the Harms Principle in the APEC Information Privacy Principles articles a risk-based approach to all

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

				privacy measures, but that was not made explicit or included in the CBPR program requirements. However, note that there are some requirements to carry out risk assessments in the context of security under the CBPR.
No equivalent in EU-U.S. Privacy Shield	36	**Prior consultation**	**No Equivalent in CBPR**	
	37	**Designation of the data protection officer**		
No equivalent in EU-U.S. Privacy Shield	37(1)	*Designation of DPO* • *The Controller and Processor must designate a DPO in certain circumstances.*	**Intake Questionnaire; General (iii.) CBPR Contact Point & CBPR Program Requirements; Assessment Criteria 40** • *Applicant must provide a "Contact Point" for CBPR.* • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles,*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			including as described in its Privacy Statement.	
No equivalent in EU-U.S. Privacy Shield	37(2)	*Group of undertakings* • *A group of undertakings may appoint a single DPO provided that it is easily accessible from each establishment.*	**Intake Questionnaire; General (iii.)** **CBPR Program Requirements; Assessment Criteria 40** • *Applicant must provide a "Contact Point" for CBPR.* • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles, including as described in its Privacy Statement.*	Note that while the CBPR do not specify the scenario of appointing a single DPO for a group of undertakings, the CBPR allow for that.
No equivalent in EU-U.S. Privacy Shield	37(3)	*Single DPO for public bodies* • *A single DPO may be designated for several public authorities or bodies.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	37(4)	*Designation of DPO for representative associations* • *Controller/processor or associations and other bodies representing categories of*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		controllers/processors may designate a DPO.		
No equivalent in EU-U.S. Privacy Shield	37(5)	*Professional qualifications* • *DPO shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices and ability to fulfil the tasks outlined in Article 39.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	37(6)	*Staff or contractor as DPO* • *DPO may be a staff member of the controller/processor or a contractor.*	**No Equivalent in CBPR**	
EU-U.S. Privacy Shield Supplementary Principle 6. Self-Certification • *To self-certify to the Privacy Shield an organization must provide to the Department a contact office for the handling of complaints, access requests, and any other*	37(7)	*Publish DPO contact details* • *Controller/processor shall publish the contact details of the DPO and communicate them to the Commissioner.*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

issues arising under the Privacy Shield.				
	38	**Position of the data protection officer**		
No equivalent in EU-U.S. Privacy Shield	38(1)	*Involve DPO in data protection issues* • *Controller/processor shall ensure the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	38(2)	*Providing resources and support to DPO* • *Controller/processor shall support the DPO in performing tasks by providing necessary resources and access to personal data and processing knowledge and in maintaining expert knowledge.*	**Intake Questionnaire; General (iii.) CBPR Contact Point & CBPR Program Requirements; Assessment Criteria 40** • *Applicant must provide a "Contact Point" for CBPR.* • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles,*	Although the CBPR do not explicitly require the Applicant to provide its appointed DPO with resources to carry out its tasks, it is clear that it will have to do so.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			including as described in its Privacy Statement.	
No equivalent in EU-U.S. Privacy Shield	38(3)	*Independence of DPO* • *Controller/processor must ensure the DPO does not receive any instructions regarding the exercise of its tasks and cannot dismiss or penalize the DPO for carrying out its tasks.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	38(4)	*Availability of DPO to assist with data subject requests to exercise rights* • *Data subjects may contact the DPO with regard to all issues related to the processing of their personal data and exercise of rights.*	**CBPR Program Requirements; Assessment Criteria 40, 41 and 42** • *Applicant must have in place opportune procedures to receive, investigate and respond to privacy-related complaints.* • *Applicant must have procedures in place to ensure individuals receive a timely response to their complaints.*	
No equivalent in EU-U.S. Privacy Shield	38(5)	*Secrecy and confidentiality*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		• *DPO shall be bound by secrecy or confidentiality concerning the performance of its tasks.*		
No equivalent in EU-U.S. Privacy Shield	38(6)	*Additional DPO tasks must not conflict* • *DPO may fulfil other tasks and duties but controller/processor must ensure such tasks and duties do not result in a conflict of interest.*	**No Equivalent in CBPR**	
	39	**Tasks of the data protection officer**		
No equivalent in EU-U.S. Privacy Shield	39(1)(a)	*Inform and advise* • *DPO must inform and advise the controller/processor and employees of their obligations under data protection law.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	39(1)(b)	*Monitor compliance* • *DPO must monitor compliance with data protection law and the data protection policies of the controller/processor, including the assignment of responsibilities, awareness-raising and training of staff*	**CBPR Program Requirements; Assessment Criteria 29, 30(a), 40 and 44** • *Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with the privacy principles,*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		involved in processing operations, and related audits.	*including as described in its Privacy Statement.* • *Applicant must have procedures in place for training employees with respect to its privacy policies and procedures.* • *Applicant must ensure that its employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight.*	
No equivalent in EU-U.S. Privacy Shield	39(1)(c)	*Provide advice on DPIAs* • *DPO must provide advice where requested as regards DPIAs*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	39(1)(d)	*Cooperate with Commissioner* • *DPO must cooperate with the Commissioner*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	39(1)(e)	*Point of contact for Commissioner*	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

		• *DPO must act as the point of contact for the Commissioner on issues relating to processing, including the prior consultation referred to in Article 36.*		
No equivalent in EU-U.S. Privacy Shield	39(2)	*Risk assessment* • *DPO must, in the performance of its tasks, have due regard to the risk associated with processing operations.*	**No Equivalent in CBPR**	
No equivalent in EU-U.S. Privacy Shield	40	**Codes of conduct**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	41	**Monitoring of approved codes of conduct**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	42	**Certification**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	43	**Certification bodies**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party*	44	**General principle for transfers**	**CBPR Program Requirements; Assessment Criteria 1(c), 1(e), 8, 9, 10, 12, 13; 50** • *Under the CBPR protections generally flow with the data. Applicant must limit*	Mostly not relevant to this mapping exercise as the CBPR themselves are a transfer mechanism or condition, but the onward transfer safeguards are relevant and the CBPR

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of			*the use of the information to the intended purpose, including when disclosing data to third parties. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations apply to the recipient who is bound by them and cannot onward transfer without these protections.* • *In cases of transfers to third parties where neither due diligence nor reasonable steps to ensure compliance with CBPR obligations are possible, the controller has to explain to the Accountability Agent why that is the case and how the information will <u>nevertheless be protected as required by the CBPR</u>. One option the controller*	directly and implicitly provide onward transfer safeguards.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request. **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *The contract should make sure that the processor understands*			*has is to obtain the consent of the individual and the controller must explain to the satisfaction of the accountability agent the nature of the consent and how it was obtained. Continued applicability of all CBPR protections can only be ensured if they apply to potential onward transfers.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

whether onward transfer is allowed.				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent*	45	**Transfers on the basis of an adequacy decision**	**CBPR Program Requirements; Assessment Criteria 1(c), 1(e), 8, 9, 10, 12, 13, 50** • *Under the CBPR protections generally flow with the data. Applicant must limit the use of the information to the intended purpose, including when disclosing data to third parties. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations apply to the recipient who is bound by them and cannot onward transfer without these protections.* • *In cases of transfers to third parties where neither due diligence nor reasonable steps to ensure*	Mostly not relevant to this mapping exercise as the CBPR themselves are a transfer mechanism or condition, but the onward transfer safeguards are relevant and the CBPR directly and implicitly provide onward transfer safeguards.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.			*compliance with CBPR obligations are possible, the controller has to explain to the Accountability Agent why that is the case and how the information will nevertheless be protected as required by the CBPR. One option the controller has is to obtain the consent of the individual and the controller must explain to the satisfaction of the accountability agent the nature of the consent and how it was obtained. Continued applicability of all CBPR protections can only be ensured if they apply to potential onward transfers.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers • *The contract should make sure that the processor understands whether onward transfer is allowed.*				
EU-U.S. Privacy Shield Principle 3. Accountability for Onward Transfer • *To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take*	46	**Transfers subject to appropriate safeguards**	**CBPR Program Requirements; Assessment Criteria 1(c), 1(e), 8, 9, 10, 12, 13, 50** • *Under the CBPR, protections generally flow with the data. Applicant must limit the use of the information to the intended purpose, including when disclosing data to third parties. When disclosing it for an unrelated purpose, the controller must obtain express consent (unless an exception applies). Any limitations apply to the*	Mostly not relevant to this mapping exercise as the CBPR themselves are a transfer mechanism or condition, but the onward transfer safeguards are relevant and the CBPR directly and implicitly provide onward transfer safeguards.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of			*recipient who is bound by them and cannot onward transfer without these protections.* • *In cases of transfers to third parties where neither due diligence nor reasonable steps to ensure compliance with CBPR obligations are possible, the controller has to explain to the Accountability Agent why that is the case and how the information will nevertheless be protected as required by the CBPR. One option the controller has is to obtain the consent of the individual and the controller must explain to the satisfaction of the accountability agent the nature of the consent and how it was obtained. Continued applicability of all CBPR protections can only be*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the relevant privacy provisions of its contract with that agent to the Department upon request. **EU-U.S. Privacy Shield Supplemental Principle 10. Obligatory Contracts for Onward Transfers** • *The contract should make sure that the processor understands whether onward transfer is allowed.*			*ensured if they apply to potential onward transfers.*	
No equivalent in EU-U.S. Privacy Shield	47	**Binding corporate rules**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
N/A	48	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	49	**Derogations for specific situations**	**CBPR Program Requirements; Assessment Criteria 50** • *Applicant may disclose personal information to other recipient persons or organizations where due diligence and reasonable*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			steps to ensure compliance with the CBPR by the recipient is impractical or impossible by explaining why such due diligence and reasonable steps for accountable transfers are impractical and impossible to perform and the other means for ensuring that the information is, nevertheless, protected consistent with the APEC Privacy Principles.	
EU-U.S. Privacy Shield Framework Overview • *The U.S. Department of Commerce issued the Privacy Shield Principles under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with the European Commission,*	50	**International cooperation for the protection of personal data** • *Commissioner shall take appropriate steps to develop international cooperation mechanisms to facilitate effective enforcement of data protection legislation, provide mutual assistance in the enforcement of such legislation, engage stakeholder in discussion and activities aimed at furthering international cooperation in*	**The APEC Cross-border Privacy Enforcement Arrangement (CPEA)** was created to ensure cross-border enforcement cooperation of the CBPR among participating economies. It enables enforcement cooperation on all data protection and privacy-related enforcement matters, not just CBPR enforcement.	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union.		*enforcement and promote the exchange and documentation of personal data protection legislation and practice.*		
No equivalent in EU-U.S. Privacy Shield	51	**Monitoring the application of this Regulation**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	52	**Independence**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
N/A	53	Deleted from UK GDPR	N/A	N/A
N/A	54	Deleted from UK GDPR	N/A	N/A
N/A	55	Deleted from UK GDPR	N/A	N/A
N/A	56	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	57	**Tasks**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	58	**Powers**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	59	**Activity reports** • *Each supervisory authority must prepare an annual report that includes types of notified infringements and measures taken.*	**Accountability Agent APEC Recognition Application; Recognition Criteria [Dispute Resolution Process - 10(g) (Accountability Agent Complaint Statistics) and (h) (Accountability Agent Case Notes)]** • The Accountability Agents must prepare annual	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

			complaint statistics and anonymized case notes on resolved CBPR complaints.	
N/A	60	Deleted from UK GDPR	N/A	N/A
N/A	61	Deleted from UK GDPR	N/A	N/A
N/A	62	Deleted from UK GDPR	N/A	N/A
N/A	63	Deleted from UK GDPR	N/A	N/A
N/A	64	Deleted from UK GDPR	N/A	N/A
N/A	65	Deleted from UK GDPR	N/A	N/A
N/A	66	Deleted from UK GDPR	N/A	N/A
N/A	67	Deleted from UK GDPR	N/A	N/A
N/A	68	Deleted from UK GDPR	N/A	N/A
N/A	69	Deleted from UK GDPR	N/A	N/A
N/A	70	Deleted from UK GDPR	N/A	N/A
N/A	71	Deleted from UK GDPR	N/A	N/A
N/A	72	Deleted from UK GDPR	N/A	N/A
N/A	73	Deleted from UK GDPR	N/A	N/A
N/A	74	Deleted from UK GDPR	N/A	N/A
N/A	75	Deleted from UK GDPR	N/A	N/A
N/A	76	Deleted from UK GDPR	N/A	N/A
EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement *Recourse Mechanisms for Individuals*	77	**Right to lodge a complaint with the Commissioner** • *Every data subject has the right to lodge a complaint with a supervisory authority.*	**CBPR Policies, Rules and Guidelines, paragraphs 22, 24, 25 and 26; Accountability Agent APEC Recognition Application; Recognition Criteria (Dispute Resolution Process - 9 and 10)**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Consumers have the ability to take complaints to independent recourse mechanisms (dispute resolution bodies), but Supplemental Principle 11 also states that consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms.* • *An arbitration option is available to an individual in the case of any residual claims not resolved by any of the other available mechanisms, if any. Arbitration may be used to determine whether a Privacy Shield organization has violated its obligations*		• *The supervisory authority must inform the complainant on the progress and outcome of the complaint, including the possibility of a judicial remedy pursuant to Article 78.*	• *For purposes of questions and complaints, the APEC CBPR Compliance Directory (www.cbprs.org) identifies and links to the relevant Privacy Enforcement Authority with jurisdiction over the Accountability Agent that certified the company that is subject of a complaint (Paragraph 22).* • *The CBPR must be enforceable by the Accountability Agents and Privacy Enforcement Authorities (Paragraph 24).* • *The CBPR system has an enforcement cooperation arrangement between the Privacy Enforcement Authorities in the participating countries (The Cross-border Privacy Enforcement Arrangement*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

under the Privacy Shield Principles as to that individual, and whether any such violation remains fully or partially unremedied. *<u>FTC Action</u>* • *The FTC reviews referrals alleging non-compliance with the Privacy Shield Principles received from: (i) privacy self-regulatory organizations and other independent dispute resolution bodies; (ii) EU Member States; and (iii) the Department, to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated.* • *Non-compliance also includes false claims of adherence to the*			*(CPEA)) (Paragraph 25 and 26).* • *The Accountability Agent must have a mechanism to receive and investigate complaints and resolve disputes (Criterion 9)* • *The dispute resolution process must include a process, inter alia, for notifying the complainant of the complaint resolution (Criterion 10)*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Privacy Shield Principles or participation in the Privacy Shield by organizations, which either are no longer on the Privacy Shield List or have never self-certified to the Department.				
No direct equivalent in EU-U.S. Privacy Shield. The Privacy Shield contains independent recourse mechanisms for individuals, including binding arbitration (see Privacy Shield criteria corresponding to GDPR articles 77 and 82).	78	**Right to an effective judicial remedy against the Commissioner**	**No Equivalent in CBPR**	The availability of this remedy depends on the domestic law of the country in which the applicant is certifying to CBPR. **FFD**
No direct equivalent in EU-U.S. Privacy Shield. The Privacy Shield contains independent recourse mechanisms for individuals, including binding arbitration (see Privacy Shield criteria	79	**Right to an effective judicial remedy against a controller or processor**	**No Equivalent in CBPR**	The availability of this remedy depends on the domestic law of the country in which the applicant is certifying to CBPR. **FFD**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

corresponding to GDPR articles 77 and 82).				
No equivalent in EU-U.S. Privacy Shield	80	**Representation of data subjects**	**No Equivalent in CBPR**	The availability of this remedy depends on the domestic law of the country in which the applicant is certifying to CBPR. **FFD**
N/A	81	Deleted from UK GDPR	N/A	N/A
EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement and Annex I *<u>Arbitration</u>* • *In arbitration, the Privacy Shield Panel has the authority to impose individual-specific, non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question) necessary to remedy the violation of the Principles only with*	82	**Right to compensation and liability**	**Not Equivalent in the CBPR but consider Accountability Agent APEC Recognition Application; Recognition Criteria (Mechanism for Enforcing Program Requirements - 13(e))** • *The Accountability Agent has a range of options in enforcing the CBPR program requirements where the certified organization has failed to remedy a violation as ordered by an Accountability Agent, including by issuing a "monetary penalty".*	Under the CBPR, it is not clear if monetary penalties by the Accountability Agent refers to penalties that may be awarded to individuals or only levied against the organization. **FFD**

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

respect to the individual. • *In considering remedies, the arbitration panel is required to consider other remedies that already have been imposed by other mechanisms under the Privacy Shield. No damages, costs, fees, or other remedies are available. Each party bears its own attorney's fees.* • *Individuals and Privacy Shield organizations will be able to seek judicial review and enforcement of the arbitral decisions pursuant to U.S. law under the Federal Arbitration Act.* *FTC Action*			• *The availability of Court ordered compensation would be subject to domestic law.*	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Consent order: If the FTC concludes that it has reason to believe that an organization violated Section 5 of the FTC Act, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in a federal district court, which if successful could result in a federal court order to same effect.* • *Civil penalty: The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order.*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

No direct equivalent in EU-U.S. Privacy Shield. However, in obtaining civil penalties for violations of consent orders, the FTC must show that the violator had "actual knowledge that such act or practice is unfair or deceptive and is unlawful" under Section 5(a)(1) of the FTC Act (*see* FTC Act Section 5(m)(1)(B), 15 U.S.C. Sec. 45(m)(1)(B)).	83	**General conditions for imposing administrative fines**	**No Equivalent in CBPR program requirements but consider Accountability Agent APEC Recognition Application; Recognition Criteria (Mechanism for Enforcing Program Requirements - 13(e))** *The Accountability Agent has a range of options in enforcing the CBPR program requirements where the certified organization has failed to remedy a violation as ordered by an Accountability Agent, including by issuing a "monetary penalty".*	Accountability agents can impose monetary penalties as deemed appropriate in their CBPR program. To our knowledge, no Accountability Agent has implemented that remedy to date. Note, however, that (outside of the CBPR program requirements) administrative fines and penalties as described in the GDPR are subject to the domestic law of the participating CBPR country and are enforceable by privacy enforcement authorities in those jurisdictions.
EU-U.S. Privacy Shield Supplemental Principle 11. Dispute Resolution and Enforcement • *If an organization persistently fails (as detailed in section (g)(ii)) to comply with the Principles, it is no*	84	**Penalties**	**No Equivalent in CBPR**	

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

longer entitled to benefit from the Privacy Shield. The organization will be removed from the Privacy Shield List and must return or delete the personal information it received under the Privacy Shield.				
EU-U.S. Privacy Shield Supplementary Principle 2. Journalistic Exceptions • *Where the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations.*	85	**Processing and freedom of expression and information**	**No Equivalent in CBPR**	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Privacy Shield Principles.*				
EU-U.S. Privacy Shield Supplemental Principle 15. Public Record and Publicly Available Information • *It is not necessary to apply the Access Principle to public record information as long as it is not combined with other*	86	**Processing and public access to official documents**	**No Equivalent in CBPR**	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

personal information (apart from small amounts used to index or organize the public record information); however, any conditions for consultation established by the relevant jurisdiction are to be respected. In contrast, where public record information is combined with other non-public record information (other than as specifically noted above), an organization must provide access to all such information, assuming it is not subject to other permitted exceptions.				
EU-U.S. Privacy Shield Framework Overview	86 A	**Processing and national security and defence**	**No Equivalent in CBPR**	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

• *Adherence to the Privacy Shield Principles may be limited to the extent necessary to meet national security, public interest, or law enforcement requirements.*				
N/A	87	Deleted from UK GDPR	N/A	N/A
N/A	88	Deleted from UK GDPR	N/A	N/A
EU-U.S. Privacy Shield Principle 5. Data Integrity and Purpose Limitation • *Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer*	89	**Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**	**CBPR Program Requirements; Assessment Criteria 26, 27, 28, 29, 39, 31, 32, 33, 34, 35 & 39** • *To the extent that CBPR certified companies engage in such data uses (i.e. processing for archiving purposes in the public interest, scientific or historical research purposes or statistical research purposes), the security safeguards and accountability requirements of the CBPR will apply.*	Not relevant to this mapping exercise

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision. **EU-U.S. Privacy Shield Framework Overview** • *Adherence to the Privacy Shield Principles may be limited: (a) to*				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided				

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

such exceptions or derogations are applied in comparable contexts.				
N/A	90	Deleted from UK GDPR	N/A	N/A
N/A	91	Deleted from UK GDPR	N/A	N/A
N/A	92	Deleted from UK GDPR	N/A	N/A
N/A	93	Deleted from UK GDPR	N/A	N/A
No equivalent in EU-U.S. Privacy Shield	94	**Repeal of Directive 95/46/EC**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	95	**Relationship with Directive 2002/58/EC**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
No equivalent in EU-U.S. Privacy Shield	96	**Relationship with previously concluded Agreements**	**No Equivalent in CBPR**	Not relevant to this mapping exercise
N/A	97	Deleted from UK GDPR	N/A	N/A
N/A	98	Deleted from UK GDPR	N/A	N/A
N/A	99	Deleted from UK GDPR	N/A	N/A

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

APPENDIX A: UK Data Protection Act 2018 – Provisions Not Appearing in the UK GDPR

Special categories of personal data and criminal conviction etc. data	S.10 and Schedule 1 Parts 1, 2 and 3 provide additional grounds for processing such data, subject to specified conditions and safeguards. S.11(1) applies further supplementary conditions to the processing of certain categories of such data.
Automated decisions required or authorized by law	S.14 applies obligations to notify data subjects of such decisions within a specified time and supplementary obligations in respect of re-considering the decision, giving further notice etc.
Conditions applicable to reliance on exemptions under Article 23	S.15 and Schedules 2, 3 and 4 implement exemptions permissible under Article 23 UK GDPR. Such exemptions are subject to certain supplementary conditions set out in the specific exemptions. Comment – the relevant point is that exemptions are specific and curtailed so they meet the criteria of being limited and specific. Broad or unrestricted exemptions would not be compatible with the UK DPA.
Processing for archiving, research and statistical purposes	S. 19 imposes additional safeguards in respect of such processing.
Enforcement	Part 6 S.142 to 164 implement the powers of the Commissioner to take enforcement actions (fines, notices, audits etc.). All the powers are subject to restrictions and conditions which impose procedural rules of fairness in the exercise of such powers. Comment – the relevant point is that a system which did not incorporate respect for proper procedures and the rights of those subject to enforcement action would not be compatible with UK DPA or UK standards more generally. The same applies to rights of appeal and other procedural matters.
Prohibitions and criminal offences	S.170 makes the unlawful obtaining or disclosure of personal data a criminal offence. S.171 makes the re-identification of de-identified data a criminal offence. S.173 makes the alteration of personal data to thwart disclosure under subject access a criminal offence. S.184 makes enforced subject access a criminal offence.

This report was produced by CIPL in connection with our work on promoting responsible global data flows and interoperability between privacy and accountability frameworks. For more information, please contact Bojana Bellamy, bbellamy@huntonak.com; Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com at the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Notes

There are further obligations on the Commissioner which are not replicated in the APEC Framework or the Privacy Shield.

- In respect of codes of practice the Commissioner must prepare and issue codes covering Age Appropriate Design, Data Protection and Journalism, Direct Marketing and Data Sharing. Once such codes come into effect they are admissible in legal proceedings so, to that extent, operate as a "soft law" part of the UK regime.

- There are also obligations to maintain a register of national security certificates, provide guidance about the application of Police and Criminal Evidence codes of practice to the Commissioner's investigations, provide guidance on redress against media organization, provide assistance to data subjects, where appropriate, in cases related to journalism and issue guidance on regulatory action.
