29 March 2018

Comments by the Centre for Information Policy Leadership

on the Article 29 Data Protection Working Party's

"Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679"

adopted on 6 February 2018

On 6 February 2018, the Article 29 Data Protection Working Party (WP) adopted its Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679 (Draft Guidelines).[1] The WP invited public comments on this document by 30 March 2018.

The Draft Guidelines provide guidance on how to interpret and implement Article 43 (certification bodies) of the GDPR, focussing mainly on the applicable standards for both National Accreditation Bodies (NABs) and Supervisory Authorities (SAs) for accrediting certification bodies under Article 43.1. The Draft Guidelines also envision an Annex containing a more detailed "framework for identifying accreditation criteria [for certification bodies]".[2] The WP has noted that the Annex will be prepared at a later stage to "take into account comments submitted in the framework of the ongoing public consultations".[3]

The Centre for Information Policy Leadership (CIPL)[4] welcomes the opportunity to submit the comments below, both as input for the WP's final Guidelines and the content of the Annex to the Guidelines. Following CIPL's 12 page submission, we attach the APEC Accountability Agent recognition criteria for the CBPR and PRP systems (see Annex) which could be instructive in any process of developing an EU-wide accreditation standard for certification bodies certified by SAs.

[1] WP261 Article 29 Working Party Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679, http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877.
[2] See Footnote 1, at page 12.
[3] See WP announcement regarding public consultation deadline at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614486.
[4] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton & Williams LLP and is financially supported by the law firm and 59 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton & Williams.

As discussed in greater detail in CIPL's earlier white paper on this topic,[5] GDPR certifications will be important to both controllers and processors of all sizes. They can be used to demonstrate compliance with the GDPR within the EU, function as cross-border transfer mechanism under the GDPR and enable "interoperability" with other, similar certifications and accountability schemes in other countries and regions. CIPL's white paper on certifications also noted that certification mechanisms should be based on a harmonised EU-wide minimum certification standard or template that is flexible and adaptable to different contexts, as well as scalable to organisations of all sizes, consistent with the mandate in Article 42(1). How certification bodies are accredited under the GDPR is directly relevant to this issue.

CIPL underlines that the GDPR provides for more than one route towards an appropriate accreditation standard: one that builds on an existing system of NABs that operate under established ISO standards, and one for SAs allowing for greater flexibility. The availability of more than one system reflects the need for scalability, which is a key requirement for the accountability mechanisms in the GDPR. Accreditation by NABs will be particularly attractive for larger organisations which are used to working with certifications in various contexts, whereas accreditation by SAs will make accreditations and certifications more broadly accessible to micro, small and medium-sized enterprises.

Accreditations by SAs are new in the GDPR. Their success depends on the following critical factors:

- SA accreditation should be based on an appropriate EU-wide baseline accreditation standard or template to avoid national fragmentation;

- The EU-wide baseline accreditation standard or template may "be guided by" but should not have to strictly follow the ISO 17065 standard; and

- The standard should maximise the potential interoperability with similar scalable certification schemes around the world.

CIPL believes that both routes towards accreditation of certification bodies will have useful roles to play within their respective areas of core competency without compromising functional consistency between them, as further explained below.

Thus, with a few clarifications as suggested below, we believe that the Draft Guidelines may facilitate the creation of effective and widely used GDPR certifications.

[5] CIPL Discussion Paper on "Certifications, Seals and Marks under the GDPR and their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms", 12 April 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

Summary of CIPL Recommendations

- When SAs accredit certification bodies pursuant to Article 43.1(a), the preference should be that they do so under a common EU-wide accreditation standard approved by the EDPB, taking into account, where relevant, the requirements adopted by the Commission in accordance with Article 43(8) GDPR.
- The EDPB should establish independent assessment criteria for reviewing SA-submitted accreditation criteria to maintain comparability and consistency across the EU, in line with Article 70(1)(o) GDPR.
- SAs and/or the EDPB and/or the Commission should not be required to strictly follow ISO 17065 as they develop or approve accreditation requirements for certification bodies under Article 43 GDPR. ISO 17065 should be viewed as instructive and useful for guidance, but not mandatory.
- The APEC Accountability Agent[6] Recognition Criteria are a good model for consideration in connection with accreditation standards to be developed by the SAs, the EDPB or the Commission.
- The forthcoming Annex to the accreditation guidelines (announced by the Draft Guidelines) setting forth guidelines on "how to identify additional accreditation criteria" should: (1) bear in mind the need for flexibility and scalability in light of the relevant GDPR mandate as discussed in CIPL's comments; (2) consider the EU Commission's policy goal of working towards cross-border convergence and interoperability with respect to similar transfer mechanisms; and (3) take guidance from the APEC Accountability Agent Recognition Criteria.
- When considering to what extent the ISO standard should "guide" the accreditation standards developed by the SAs and EDPB, relevant international experience dealing with certifications under ISO conformity assessments should be considered where the ISO standards have failed to ensure scalability and affordability for purposes of micro, small and medium-sized enterprises.
- The ISO 17065 standard should also be applied flexibly by the NABs to further the scalability goals of the GDPR with respect to micro, small and medium-sized enterprises and to facilitate consistency with the standard(s) developed or approved by the SAs or the EDPB or the Commission.
- The "additional requirements" the SAs develop for accreditations by NABs under Article 43.1(b) should also take into account scalability and the needs of micro, small and medium-sized enterprises.

[6] The term "Accountability Agents" in the APEC CBPR and PRP systems refers to the third-party certification organisations that provide CBPR or PRP certifications to companies.

Discussion

I. Key GDPR provisions

The GDPR certification scheme requires the existence of certification bodies that have been formally accredited to issue certifications to organisations. According to Article 43.1(a) and (b), certification bodies may be accredited by:

(1) the competent supervisory authority (SA);

(2) the national accreditation body (NAB); or

(3) by both.[7]

Article 43.1(b) provides that the NABs[8] must accredit certification bodies "in accordance with EN-ISO/IEC 17065/2012 (ISO 17065) and with additional requirements established by the supervisory authority which is competent pursuant to Article 55 and 56" (Emphasis added).[9]

The GDPR does not require the SAs to rely on ISO 17065 when they accredit certification bodies; such requirement is only for NABs. Nor does the GDPR otherwise define a specific standard to be employed by the SA during the accreditation process, other than a list of general criteria for certification bodies in Article 43.2 that apply to accreditation by both an SA or an NAB. These criteria include independence, subject matter expertise, having approved certification criteria and procedures, and an absence of a conflict of interest.

Article 43.3, read together with Article 64.1, provides that accreditation of certification bodies by an SA shall take place on the basis of criteria approved by that SA, subject to an opinion by the EDPB, or by the EDPB itself pursuant to Article 63 (consistency mechanism). Article 43.3 also reiterates that accreditation of certification bodies by NABs shall be based on the criteria approved by the SA,[10] which will complement the requirements envisaged in Regulation (EC) No. 765/2008 and the ISO 17065 standards (i.e. "the technical rules that describe the methods and procedures of the certification bodies", Art. 43.3).[11] However, as noted, the accreditation by SAs does not have to be in accordance with ISO 17065. As such, SA accreditations can be more flexible in their requirements and criteria than NAB accreditations.

---

[7] See Footnote 1, at page 8.
[8] NABs must also be "named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council" setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218/30. Article 43.1(b).
[9] See Footnote 1, at page 9.
[10] The phase "those requirements" in Article 43.3 refers to the criteria developed by the supervisory authorities and the requirements set out in Article 43.2. Draft Guidelines, p. 9.
[11] See Footnote 1, at Section 4.3, page 9.

II. Purpose of the Draft Guidelines

Noting the important role certifications can play to "enhance compliance with the GDPR and transparency for data subjects and in B2B relations, for example between controllers and processors", the WP states that the purpose of the Draft Guidelines is "to provide guidance on how to interpret and implement the provisions of Article 43 of the GDPR" and to "help Member States, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR".[12]

The Draft Guidelines address several issues, two of which[13] will be the focus of CIPL's comment:

> (1) providing a framework for establishing the "additional" accreditation requirements (in addition to ISO 17065) under Article 43.1(b) when the accreditation is handled by a NAB; and
>
> (2) providing a framework for establishing accreditation requirements for when the accreditation is handled by the SA.

III. Scalability as an overarching requirement of GDPR certifications

The overarching question in this context is to what extent the applicable accreditation criteria for certification bodies facilitate the GDPR's mandate that certifications be scalable and available to micro, small and medium-sized companies.[14] Such companies make up a large portion of the data ecosystem.

As mentioned, the ability to obtain GDPR certifications will be of significant value to organisations of all sizes. In addition to serving as both a general compliance tool and a cross-border transfer mechanism, certification will be particularly relevant to organisations choosing a trusted, certified data processor. Under Article 28.5 of the GDPR, the certification of a data processor can be used as "an element by which to demonstrate sufficient guarantees" of GDPR compliance, i.e. as a "due diligence" tool for controllers. Thus, certification will provide a significant benefit both to controllers seeking to retain processor services and to processors trying to demonstrate their accountability and differentiate themselves through certification from the rest of the market. But for this benefit to become broadly attainable, certifications must be widely available and affordable.

---

[12] See Footnote 1, at page 4 (Emphasis added).

[13] See Footnote 1, at page 5.

[14] Article 42(1) provides that "[t]he Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account". (Emphasis added)

While certainly valuable and beneficial within their sphere of competency, ISO standards do not have a known track record of broad applicability for SMEs. The relevant data protection stakeholders, most notably the SAs and EDPB, should, therefore, devise a scalable accreditation and certification system that is suitable for the data protection context. Overly restrictive and cost-prohibitive accreditation standards will limit the range of available certification bodies in the ecosystem and will act as a barrier to entry for many certification bodies, as further discussed below. The lack of accredited certification bodies may lead to less choice and higher cost and, ultimately, may limit the number of certified organisations. Thus, together with the appropriate rigour, scalability and affordability must be priority considerations when developing accreditation criteria for certification bodies.

IV. Accreditations by the National Accreditation Bodies and the Supervisory Authority

It is critical to the successful uptake of GDPR certifications that a wide range of certification bodies can become accredited. Article 43.1, in fact, enables this by not limiting such accreditations to NABs but by also allowing SAs (and the EDPB) to develop separate accreditation requirements that can be specifically designed to address the scalability mandate in Article 42.1.

This additional route towards accreditation is particularly important as Regulation (EC) No. 765/2008 limits the number of NABs to one per Member State. This limitation, coupled with a potentially narrow accreditation standard (see discussion below), would result in limited numbers of certification bodies and certified companies.

Moreover, it remains to be seen whether the product-based scheme under Regulation (EC) No. 765/2008 will be effective in the novel context of an Article 42 certification applicable to a broad range of data processing operations. Thus, in order to maximise the range of organisations that are able to be certified (and in consideration of issues of scalability that are especially important to micro, small and medium-sized enterprises), it makes sense for the GDPR to allow SAs to develop accreditation standards based on EDPB-developed guidance and a model or template designed by the EDPB specifically for the specialised context of Article 42 privacy certifications with selective reference to ISO 17065 where appropriate. Such a model or template baseline accreditation standard developed by the EDPB would ensure consistency and mutual recognition between the accreditations by the SAs as well as maintain an appropriate level of consistency with the accreditation standards applicable to the NABs, as further discussed below. Requirements that may potentially be adopted by the Commission in accordance with Article 43.8 could also add value on this point. Moreover, to the extent such a standard can be developed taking into account the recognition criteria for certification bodies of other systems (such as the APEC CBPR and PRP), it would enable global interoperability and consistency as well. See discussion in Section VI below.

Indeed, the WP notes the absence of specific instructions in the GDPR on the criteria SAs must include in their accreditation requirements (other than the ones set forth in Article 43.2). This is in contrast to the more specific instructions pertaining to the accreditation criteria to be applied by the NABs. The fact that the GDPR does not set forth the same criteria for SA and NAP accreditation suggests the drafters' intent that the standards not be identical—as well as more flexibility granted to the SAs in exercise of their independent authority. However, the WP nevertheless concludes that "in the interest of contributing to a harmonized approach to accreditation" between the supervisory authorities and the national accreditation bodies, "the accreditation criteria used by the supervisory authority should be guided by ISO 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43.1(b)".[15]

CIPL agrees that consistency is essential to providing a trusted certification ecosystem that enables mutual recognition of the accreditation criteria for certification bodies and of the certifications the system ultimately produces. Thus, consistency between the accreditation criteria for the NABs and the SAs is a legitimate and desirable goal, but it does not require that the standards be identical. Under the GDPR, consistency cannot be at the expense of scalability and accessibility of the certifications to organisations of all sizes. It must and can be achieved by creating "functional consistency" that aligns the key elements of the relevant accreditation standards rather than focuses on wholesale adoption of one standard (the ISO standard) that may be appropriate and workable for large organisations.

Indeed, the WP's phrase "should be guided by" correctly describes the relevance of the ISO standard for the accreditation criteria to be developed by the SAs (subject to and in line with EU-wide criteria developed by the EDPB). CIPL is simply flagging the importance of properly interpreting and applying the WP's "should be guided by" characterisation. As stated, and also as further discussed below, strict adherence to the ISO standard may lead to the introduction of prohibitive burdens and costs, thereby limiting the pool of potential certification bodies entering the market. A costly accreditation process or unsustainably high liabilities of certification bodies would create a more costly certification process for controllers and processors. This may practically render Article 42 certifications unavailable to micro, small and medium-sized organisations. Thus, the meaning of the WP's above phrasing of "should be guided by ISO 17065" should be clarified in the final Guidelines as leaving room for the necessary flexibility.

[15] See Footnote 1, at page 10 (Emphasis added). The WP also points out that the accreditation criteria in Article 43.2(a)-(e) already reflect and specify requirements of ISO 17065, noting that this will also contribute to consistency.

V. ISO 17065

ISO 17065 sets forth standards for "Conformity assessment – Requirements for bodies certifying products, processes and services", which are provided in eight sections and numerous subsections.[16] While under the GDPR the national accreditation bodies must accredit certification bodies "in accordance" with ISO 17065, the Draft Guidelines suggest that the SAs should also "be guided" by that standard. However, due to the nature of the ISO 17065 standard, a strict application of that standard could result in limited numbers of certification bodies and, ultimately, few certified organisations. The examples below demonstrate why that is the case. Thus, CIPL recommends the development of stand-alone GDPR-specific certification standards by the SAs (or the EDPB) with only selective reference to additional ISO standards where appropriate. To the extent the SAs (or the EDPB) look to the ISO standards in their own accreditation standards developed pursuant to Articles 43.1 and 43.3, the selection and phrasing should be done with an eye to enabling scalability and sufficient flexibility so that smaller certification bodies can be accredited.

Several examples from ISO 17065 cited below illustrate the potential negative effects of adopting the ISO standard in its entirety and/or without appropriate clarification and interpretation.

Example 1: **Section 4.3 on "Liability and Financing"**

Section 4.3.1 provides that "[t]he certification body shall have adequate arrangements (e.g. insurance or reserves) to cover liabilities from its operations".

This provision will have the effect of excluding potential certification bodies from being accredited, depending on how it is interpreted. As to the ability to "cover liabilities from its operations", for this section to be workable in the GDPR certifications context, it should be interpreted to apply to a certification body's ability to cover its general commercial liabilities. Liability should not be interpreted to include potential administrative fines for violations of the GDPR itself. This inclusion would effectively prohibit all but the very largest entities from serving as a certification body and functionally preclude most entities operating under a non-profit corporate structure. At the very least, the Working Party should clarify this in its guidelines.[17]

It is also unclear how this requirement would apply to SAs that choose to act as certification bodies, which indicates that the ISO standard, by definition, cannot be applied comprehensively to certifications provided by supervisory authorities.

[16] As mentioned and noted by the WP, Article 43.2—which applies to accreditations both by national accreditation bodies and SAs—already incorporates some elements of ISO 17065.

[17] In addition to the point that only general commercial liability should be covered under Section 4.3, certification bodies should only be liable for their own violations and not those of the organisations they certified. A good example might be the model followed by accounting firms, which do not accept liability for any misrepresentations in the financial statements of their clients.

There is some relevant international experience on privacy certifications in the context of conformity assessment. A notable case is Mexico, where Binding Self-Regulation parameters based on Mexican law equivalents of ISO 17065 were issued by the Mexican Data Protection Authority in 2014. These include similar requirements for certification and standardisation bodies. The result of the incorporation of ISO 17065 has been a very limited uptake by industry. To date only one certification and one standardisation body have been accredited.[18] Indeed, the anecdotal evidence from the Mexican experience suggests that the need to comply with overly prescriptive conformity assessment and normalisation requirements will exclude many organisations from becoming certifiers. That in turn concentrates the certification in a single authority and may increase the cost to the companies that seek certification.

Example 2: **Section 6.2 on "Resources for Evaluation"**

Section 6.2.1 provides that

> "[w]hen a certification body performs evaluation activities, either with its internal resources or with other resources under its direct control, it shall meet the applicable requirements of the relevant International Standards and, as specified by the certification scheme, of other documents. For testing, it shall meet the applicable requirements of ISO/IEC 17025; for inspection, it shall meet the applicable requirements of ISO/IEC 17020; and for management system auditing, it shall meet the applicable requirements of ISO/IEC 17021. The impartiality requirements of the evaluation personnel stipulated in the relevant standard shall always be applicable".

Strict adherence to ISO 17065 would necessarily require the introduction of additional ISO standards which may have limited utility in the performance of a GDPR-based privacy certification (e.g. ISO 17025 is designed to apply to the testing and/or calibration activities of laboratories). Further, the prescriptive application of requirements that are not specifically designed to address the unique nature of a GDPR-based privacy certification complicates the accreditation process and ultimately undermines the scalability goals of the GDPR and the harmonisation the WP guidance intends to foster.

Example 3: **Sections 7.4 - 7.6 "Review, Evaluation and Certification Decision"**

Section 7.4.2 provides that "[t]he certification body shall assign personnel to perform each evaluation task that it undertakes with its internal resources (see 6.2.1)".

Section 7.5.1 further provides that "[t]he certification body shall assign at least one person to review all information and results related to the evaluation. The review shall be carried out by person(s) who have not been involved in the evaluation process".

[18] More information can be found here: http://rea.inai.org.mx/_catalogs/masterpage/Sec6_1.aspx.

Finally Section 7.6.2 provides that "[t]he certification body shall assign at least one person to make the certification decision based on all information related to the evaluation, its review, and any other relevant information. The certification decision shall be carried out by a person or group of persons [e.g. a committee (see 5.1.4)] that has not been involved in the process for evaluation (see 7.4)".

Taken together, Sections 7.4 - 7.6 introduce a multiple-step certification process that would, in effect, increase both the time and the costs associated with an Article 42 certification. We suggest that quality control can be effectively achieved through the development of the additional privacy-specific accreditation criteria contemplated by Article 43.2 (i.e. independence, subject matter expertise, having approved certification criteria and procedures, and an absence of a conflict of interest). Further, reliance on one set of criteria developed specifically for an Article 42 certification (though "guided by" the ISO standard where appropriate) would promote procedural harmonisation for accreditations by SAs, as well as sufficient consistency between SAs and NABs.

Example 4: **Section 7.9 on "Surveillance"**

Section 7.9.4 provides that

> "[w]hen continuing use of a certification mark is authorized for a process or service, surveillance shall be established and shall include periodic surveillance activities to ensure ongoing validity of the demonstration of fulfilment of process or service requirements".

Here it is critical that the concept of "surveillance" be given a reasonable and pragmatic interpretation that grants certification bodies sufficient discretion and flexibility to determine the appropriate level of ongoing monitoring, as well as the appropriate tools. Without such discretion and flexibility, this standard could easily result in unnecessary and disproportionate monitoring activities that will make providing certification services cost prohibitive to potential smaller certification bodies as well as to their customers. Again, this is an example of a criterion that must be applied in light of the GDPR mandate to make certifications accessible and scalable. Article 43.2(c) of the GDPR requires certification bodies to have "established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks" (Emphasis added). Periodic review does not equal surveillance. Surveillance implies a more structured and deeper requirement than a periodic review (which encompasses "spot checking") and suggests a continuous process. Thus, to avoid the potentially debilitating impacts of such a process on the scalability of a GDPR certification system, there clearly is a need to apply Article 43.2(c) ("periodic review") instead of the requirement in ISO 17065 Section 7.9.4.

VI. ISO 17065 and the APEC Accountability Agent Recognition Criteria

In the APEC Cross-Border Privacy Rules (CBPR) and APEC Privacy Recognition for Processors (PRP) systems, certification bodies are called "Accountability Agents" (AAs). APEC has developed a comprehensive set of formal recognition criteria that APEC AAs must meet.[19] The APEC AA recognition criteria represent a rigorous yet flexible and scalable set of standards for AAs that could be instructive to both EU SAs and the EDPB in any process of developing an EU-wide accreditation standard for certification bodies certified by SAs. Importantly, there is substantial overlap and parity with respect to the essential accreditation or recognition criteria in both systems. In some cases, such as for example in connection with ISO 17065 Section 7.9.4 (regarding "surveillance"), the APEC correlate may be a useful example of how the same concept can be expressed in a way that reflects the necessary flexibility (i.e. "surveillance" (ISO) vs. "monitoring" and "review" upon notice of a possible violation (APEC)) .

As we noted in CIPL's earlier discussion paper on GDPR certifications,[20] to facilitate EU-wide harmonisation and global interoperability, there should be a preference for one EU baseline certification for all contexts and sectors, with possible differentiation in its application, i.e. a "common certification" or "European Data Protection Seal" under Article 42.5 of the GDPR, developed under the lead of the Commission or the EDPB in collaboration with certification bodies and industry.[21] Similarly, there should be a common baseline accreditation standard approved by the EDPB under Article 64 (or the Commission under Article 43.8) for certification bodies accredited by the SAs. As discussed above, this baseline standard would ensure appropriate and functional intra-EU consistency across the various SAs that will be accrediting certification bodies under Article 43.1(a) and between the SAs and the NABs, as well as enable global consistency and interoperability with other systems.

Indeed, the Draft Guidelines note that "Member States and supervisory authorities should keep in mind the harmonised European level when formulating national law and procedures relating to accreditation and certification in accordance with the GDPR".[22] Ultimately, such a common EU-wide approach to accreditation of certifications bodies that is developed with scalability and flexibility in mind will not only enable the express

[19] Accountability Agent – APEC Recognition Application (includes the recognition criteria), attached as Annex 1 hereto, available also at https://cbprs.blob.core.windows.net/files/Accountability%20Agent%20Application%20for%20CBPR%20Revised%20For%20Posting%203-16.pdf. See also the APEC recognition criteria for the PRP, which are identical as for the CBPR. They are available at https://www.apec.org/~/media/Files/Groups/ECSG/2015/Accountability%20Agent%20Application%20for%20the%20PRP%20System.pdf.

[20] See Footnote 5.

[21] Thus, there may be many certification schemes in the EU, but they would be pegged to the same EU-wide baseline GDPR standard and would differ only in their context- or industry-specific adaptations. See CIPL's white paper on certifications for details.

[22] See Footnote 1, at page 11.

goals of the GDPR but also the EU Commission's stated policy of promoting convergence or interoperability with non-EU cross-border transfer standards and systems, such as the APEC CBPR.[23]

Conclusion

CIPL is grateful for the opportunity to provide comments on key implementation questions regarding the accreditation standards for certification bodies. We look forward to providing further input as the relevant accreditation standards are being developed, as well as to contributing generally to the development of effective and scalable GDPR certifications.

If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@hunton.com; Markus Heyder, mheyder@hunton.com; or Sam Grogan, sgrogan@hunton.com.

[23] See CIPL's discussion paper on certifications under the GDPR, Footnote 5 supra, discussing the Communication from the Commission to the European Parliament and the Council; Exchanging and Protecting Personal Data in a Globalised World, Brussels 10.1.2017, COM (2017) 7 final (Emphasis added), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=41157.

ANNEX

Asia-Pacific
Economic Cooperation

ACCOUNTABILITY AGENT APEC RECOGNITION APPLICATION

OVERVIEW

The purpose of this document is to guide the application process for Accountability Agents seeking APEC recognition under the APEC Cross Border Privacy Rules (CBPR) System. This document explains the necessary recognition criteria and provides the baseline program requirements of the CBPR System. Only APEC-recognized Accountability Agents may participate in the CBPR System. Once recognized, Accountability Agents may publicize this recognition and certify organizations as CBPR compliant. A recognized Accountability Agent would only be able to certify as CBPR compliant those organizations that are subject to the enforcement authority of CPEA-participating privacy enforcement authorities within the economies in which it has been approved to operate.

APPLICATION PROCESS

In order to be considered eligible for recognition by APEC Economies, an Applicant Accountability Agent must:

- Explain how it is subject to the jurisdiction of the relevant enforcement authority in a CBPR participating Economy[1]; *AND*
- Describe how each of the Accountability Agent Recognition Criteria (Annex A) have been met using the Accountability Agent Recognition Criteria Checklist (Annex B); *AND*
- Agree to make use of the template documentation developed and endorsed by APEC Economies (the CBPR Intake Questionnaire[2] and the CBPR Program Requirements[3]) to assess applicant organizations when certifying organizations as CBPR-compliant; *OR* demonstrate how their existing intake and review processes meet the baseline established using the CBPR Program Requirements Map (Annex C[4]) and publish their program requirements; *AND*
- Complete the signature and contact information sheet (Annex F).

The completed signature and contact information sheet and all necessary supporting documentation should be submitted to the relevant government agencies or public authorities in any Economy in which the Applicant Accountability Agent intends to operate for an initial review to ensure the necessary documentation is included in the application, or other review as appropriate. The agency or authority may consult with other government agencies or authorities where necessary and will forward all information received to the Chair of the Electronic Commerce Steering Group, the Chair of the Data Privacy Subgroup and the Chair of the Joint Oversight Panel (JOP) where appropriate. The JOP will review the submitted information (and request any additional information that may be needed) when considering recommending the Applicant Accountability Agent for recognition by APEC Economies as an APEC CBPR System Accountability Agent.

---

[1] An Economy is considered a participant in the Cross Border Privacy Rules System pursuant to the terms established in Paragraph 2.2 of the "Charter of the APEC Cross-Border Privacy Rules System Joint Oversight Panel" (*available at* http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11_ecsg2_012.pdf)

[2] *Available at* http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11_ecsg2_014.doc

[3] *Available at* http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_007.doc

[4] Annex C should be read consistently with the APEC Cross Border Privacy Rules Intake Questionnaire which lists the acceptable qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms referred to in this document.

Annex A

ACCOUNTABILITY AGENT RECOGNITION CRITERIA

CRITERIA

Conflicts of Interest

1) General Requirements:

    a. An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the APEC Cross Border Privacy Rules (CBPR) System. For the purposes of participation as an Accountability Agent in the CBPR System, this means the ability of the Accountability Agent to perform all tasks related to an Applicant organization's certification and ongoing participation in the CBPR System free from influences that would compromise the Accountability Agent's professional judgment, objectivity and integrity.

    b. An Accountability Agent must satisfy the APEC member economies with evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Such safeguards should include but not be limited to:

        i. Written policies for disclosure of potential conflicts of interest and, where appropriate, withdrawal of the Accountability Agent from particular engagements. Such withdrawal will be required in cases where the Accountability Agent is related to the Applicant organization or Participant to the extent that it would give rise to a risk that the Accountability Agent's professional judgment, integrity, or objectivity could be influenced by the relationship.

        ii. Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.

        iii. Written policies for internal review of potential conflicts of interest with Applicant organizations and Participating organizations.

        iv. Published certification standards for Applicant organizations and Participating organizations (see paragraph 4 'Program Requirements').

        v. Mechanisms for regular reporting to the relevant government agency or public authority on certification of new Applicant organizations, audits of existing Participant organizations, and dispute resolution.

        vi. Mechanisms for mandatory publication of case reports in certain circumstances.

2) Requirements with respect to particular Applicant organizations and/or Participant organizations

a. At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant organization or Participant organization that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the CBPR System, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during dispute resolution and enforcement of the Program Requirements against a Participant. Such affiliations, which include but are not limited to the Applicant organization or Participant organization and the Accountability Agent being under common control such that the Applicant organization or Participant organization can exert undue influence in the Accountability Agent, constitute relationships that require withdrawal under 1(b)(i).

b. For other types of affiliations that may be cured by the existence of structural safeguards or other procedures undertaken by the Accountability Agent, the existence of any such affiliations between the Accountability Agent and the Applicant organization or Participant organization must be disclosed promptly to the Joint Oversight Panel, together with an explanation of the safeguards in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant organization or Participant organization. Such affiliations include but are not limited to:

    i. officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;

    ii. significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the APEC CBPR System; or

    iii. all other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the CBPR System.

c. Outside of the functions described in paragraphs 5-14 of this document, an Accountability Agent will refrain from performing for its Participants or Applicants services for a fee or any interest or benefit such as the following categories:

    i. consulting or technical services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures;

    ii. consulting or technical services related to the development of its privacy policy or statement; or

iii. consulting or technical services related to its security safeguards.

d. An Accountability Agent may be engaged to perform consulting or technical services for an Applicant organization or Participant organization other than services relating to their certification and on-going participation in the CBPR System. Where this occurs, the Accountability Agent will disclose to the Joint Oversight Panel:

i. the existence of the engagement; and

ii. an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement [*such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the functions described in paragraphs 5 -14 of this document*].

e. Provision of services as required in Sections 3 through 6 shall not be considered performing consulting services which might trigger a prohibition contained in this document.

3) In addition to disclosing to the Joint Oversight Panel all withdrawals described above in Section 1(b)(i), an Accountability Agent also shall disclose to the Joint Oversight Panel those activities or business ventures identified in subsection 1(b) above that might on their face have been considered a conflict of interest but did not result in withdrawal. Such disclosures should include a description of the reasons for non-withdrawal and the measures the Accountability Agent took to avoid or cure any potential prejudicial results stemming from the actual or potential conflict of interest.

Program Requirements

4) An Accountability Agent evaluates Applicant organizations against a set of program requirements that encompass all of the principles of the APEC Privacy Framework with respect to cross border data transfers and that meet the CBPR program requirements developed and endorsed by APEC member economies (to be submitted along with this form, see Annex A). (*NOTE:* an Accountability Agent may charge a fee to a Participant for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.)

Certification Process

5) An Accountability Agent has a comprehensive process to review an Applicant organization's policies and practices with respect to the Applicant organization's participation in the Cross Border Privacy Rules System and to verify its compliance with the Accountability Agent's program requirements. The certification process includes:

a) An initial assessment of compliance, which will include verifying the contents of the self-assessment forms completed by the Applicant organization against the program requirements for Accountability Agents, and which may also

include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

b) A comprehensive report to the Applicant organization outlining the Accountability Agent's findings regarding the Applicant organization's level of compliance with the program requirements. Where non-fulfillment of any of the program requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the CBPR System.

c) Verification that any changes required under subsection (b) have been properly completed by the Applicant organization.

d) Certification that the Applicant organization is in compliance with the Accountability Agent's program requirements. An Applicant organization that has received such a certification will be referred to herein as a "Participant" in the CBPR System.

e) Provision of the relevant details of the Participant's certification for the Compliance Directory.[1] The relevant details should include at least the following: the name of the certified organization, a website for the certified organization and a link to the organization's privacy policy, contact information, the Accountability Agent that certified the Participant and can handle consumer disputes, the relevant Privacy Enforcement Authority, the scope of the certification, the organization's original certification date, and the date that the current certification expires.

On-going Monitoring and Compliance Review Processes

6) Accountability Agent has comprehensive written procedures designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent's program.

7) In addition, where there are reasonable grounds for the Accountability Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. Where non-compliance with any of the program requirements is found, the Accountability Agent will notify the Participant outlining the corrections the Participant needs to make and a reasonable timeframe within which the corrections must be completed. The Accountability Agent must verify that the required changes have been properly completed by the Participant within the stated timeframe.

Re-Certification and Annual Attestation

8) Accountability Agent will require Participants to attest on an annual basis to the continuing adherence to the CBPR program requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification. Where there has been a material change to the Participant's privacy policy (as reasonably determined by the Accountability Agent in good faith), an

[1] See "APEC Cross Border Privacy Rules System Policies, Rules and Guidelines," paragraph 14 (*available at* http://aimp.apec.org/Documents/2011/ECSG/ECSG2/11_ecsg2_012.pdf).

immediate review process will be carried out. This re-certification review process includes:

a) An assessment of compliance, which will include verification of the contents of the self-assessment forms (Project 1) updated by the Participant, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

b) A report to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification.

c) Verification that required changes have been properly completed by Participant.

d) Notice to the Participant that the Participant is in compliance with the Accountability Agent's program requirements and has been re-certified.

Dispute Resolution Process

9) 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. Such mechanism must be publicized on the Participant's website. An Accountability Agent may choose not to directly supply the dispute resolution mechanism. The dispute resolution mechanism may be contracted out by an Accountability Agent to a third party for supply of the dispute resolution service. Where the dispute resolution mechanism is contracted out by an Accountability Agent the relationship must be in place at the time the Accountability Agent is certified under the APEC CBPR system. An Accountability Agent's website must include the contact point information for the relevant Privacy Enforcement Authority. Publicizing such contact point information allows consumers or other interested parties to direct questions and complaints to the relevant Accountability Agent, or if necessary, to contact the relevant Privacy Enforcement Authority.

10) The dispute resolution process, whether supplied directly or by a third party under contract, includes the following elements:

a) A process for receiving complaints and determining whether a complaint concerns the Participant's obligations under the program and that the filed complaint falls within the scope of the program's requirements.

b) A process for notifying the complainant of the determination made under subpart (a), above.

c) A process for investigating complaints.

d) A confidential and timely process for resolving complaints. Where non-

compliance with any of the program requirements is found, the Accountability Agent or contracted third party supplier of the dispute resolution service will notify the Participant outlining the corrections the Participant needs to make and the reasonable timeframe within which the corrections must be
completed.

e) Written notice of complaint resolution by the Accountability Agent or contracted third party supplier of the dispute resolution service to the complainant and the Participant.

f) A process for obtaining an individual's consent before sharing that individual's personal information with the relevant enforcement authority in connection with a request for assistance.

g) A process for making publicly available statistics on the types of complaints received by the Accountability Agent or contracted third party supplier of the dispute resolution service and the outcomes of such complaints, and for communicating that information to the relevant government agency and privacy enforcement authority (see Annex E).

h) A process for releasing in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes (see Annex D).

Mechanism for Enforcing Program Requirements

11) Accountability Agent has the authority to enforce its program requirements against Participants, either through contract or by law.

12) Accountability Agent has a process in place for notifying Participant immediately of non-compliance with Accountability Agent's program requirements and for requiring Participant to remedy the non-compliance within a specified time period.

13) Accountability Agent has processes in place to impose the following penalties, which is proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period. [*NOTE*: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.]

a) Requiring Participant to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the Participant from its program.

b) Temporarily suspending the Participant's right to display the Accountability Agent's seal.

c) Naming the Participant and publicizing the non-compliance.

d) Referring the violation to the relevant public authority or privacy enforcement authority. [*NOTE*: this should be reserved for circumstances where a violation raises to the level of a violation of applicable law.]

e) Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

14) 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 under the procedures established by the Accountability Agent pursuant to paragraph 2 so long as such failure to comply can be reasonably believed to be a violation of applicable law.

15) Where possible, Accountability Agent will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the CBPR- related activities of the Accountability Agent.

Annex B

ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST

Conflicts of Interest

1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.

2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.

3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

Program Requirements

4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

Certification Process

5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.

On-going Monitoring and Compliance Review Processes

6. Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).

7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

Re-Certification and Annual Attestation

8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

Dispute Resolution Process

9. Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.

10. Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third

party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

Mechanism for Enforcing Program Requirements

11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.

12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.

13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].

15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

Annex C

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS MAP

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant organization's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies	

	an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	
1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.c) Does this privacy	Where the Applicant answers **YES**, the	

statement inform individuals whether their personal information is made available to third parties and for what purpose?	Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a **functional** e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.e) Does this privacy statement provide information regarding the use and disclosure of an	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all	

individual's personal information?	personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). • The process that an individual must follow in order to correct his or her personal information Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
2. Subject to the qualifications listed below,	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant	

at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
4. Subject to the	Where the Applicant answers **YES**, the	

qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: • Each type of data collected • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data • An explanation of the compatibility or relatedness of each identified use with the stated purpose of	

	collection Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require	

circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	
10. Do you disclose personal information you collect (whether directly or through the use of third	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure	

parties acting on your behalf) to other personal information controllers? If YES, describe.	and/or 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 necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	
11. Do you transfer personal information to personal information processors? If YES, describe.		
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection • Via e-mail	

applicable laws?	• Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability	

	Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service	

	Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise	

	choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which the information was collected.] Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner . Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	
18. When choices are	Where the Applicant answers **YES**, the Accountability	

provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the	

	Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax,	

attachment if necessary.	through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	
24. Where inaccurate, incomplete or out of date information will affect the	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate	

purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.	corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's	

	size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that	

	information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for	

network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	compliance with this principle.	
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	

below.		
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	

privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The 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. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals	

	in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	

communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.		
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers **YES to questions 38.a**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting	

38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations ____ • Compliance with self-regulatory applicant code and/or rules ____	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	

• Other (describe) ____		
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR	

	4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure	Where the Applicant answers **YES, the** Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the	

of personal information?	necessary training to employees regarding this subject. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies _____ • Contracts _____ • Compliance with applicable industry or sector laws and regulations _____ • Compliance with self-regulatory applicant code and/or rules _____ • Other (describe) _____	Where the Applicant answers **YES, the** Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC-	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	

compliant privacy policies and practices as stated in your Privacy Statement? _____ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ • Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ • Impose restrictions on subcontracting unless with your consent? _____ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____ • Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? • Other (describe) _____		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you	The Accountability Agent must verify the existence of such self-assessments.	

with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.		
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	
50. Do you disclose personal information to other recipient **persons or organizations** in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	

Annex D

ACCOUNTABILITY AGENT CASE NOTES

The Accountability Agent Recognition Criteria require applicants to attest that as part of their dispute resolution mechanism they have a process for releasing, in anonymised form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes.

The template, with associated guidance and FAQs, will assist in meeting the requirement.

Objectives of Release of Case Notes

Complaints handling is an important element of the Cross-border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to release case notes on a selection of resolved complaints in order to:

- promote understanding about the operation of the CBPR program;
- assist consumers and businesses and their advisers;
- facilitate consistency in the interpretation of the APEC information privacy principles and the common elements of the CBPR program;
- increase transparency in the CBPR program; and
- promote accountability of those involved in complaints handling and build stakeholder trust in accountability agents.

Commentary on the Template

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template for stylistic reasons by, for example, reordering the elements (e.g. by switching the date and citation to different ends of the note) or adding additional elements. However, it would be difficult to produce a satisfactory case note without the minimum elements mentioned in the template.

General heading

It is possible to combine the general heading and citation into a single heading or adopt a citation that stands in for a general heading. However, unlike a series of law reports directed exclusively at lawyers, case notes are useful as an educational tool for ordinary consumers and businesses. Accordingly, a general heading that communicates a clear straightforward message is recommended.

Citation

It is essential that all those that may wish to refer to a case note can do so by an accepted citation that unambiguously refers to the same note. All case notes should be issued with a citation including the following elements:

- a descriptor of the case;
- the year of publication ;

- a standard abbreviation for the accountability authority (including an indicator of which economy the Accountability Agent is based), and;
- a sequential number.

Case report

The style and approach of case reports can differ substantially but there are several elements that almost certainly will appear. These include:

- an account of the facts (e.g. as initially asserted on a complaint and as found after investigation)
- the relevant law (which will include the elements of the CBPR program)
- a discussion of the issues of interest and how the law applied to the facts in question
- the outcome of the complaint.

Key terms

It may be useful to include the standard terms used in traditional indexing or which will appear as tags in on-line environments.

CASE NOTE TEMPLATE

General heading

Citation

Case report

- Facts
- Law
- Discussion
- Outcome

Date

Key terms

- Tags

CASE NOTE FREQUENTLY ASKED QUESTIONS

Q. How many case notes should an Accountability Agent publish?

A. Those responsible for a CBPR program may find it useful to set targets for how many case notes should be published and make those targets public. In the initial years of a scheme's operation a greater number of case notes may be warranted so as to assist advisers and to provide reassurance to regulators and others. In later years, when there is a greater body of case notes available, fewer new notes may be needed. A scheme handling very few complaints will need to report a greater proportion of its complaints than a large scheme which can be more selective. As a general guide, a scheme handling more than 200 complaints a year might aim to publish about 8-10% of that number in case notes in the early years dropping later to, perhaps, 3–5 %.

Q. Which resolved complaints should be selected for case notes?

A. Those responsible for a CBPR program may find it useful to adopt standards to be applied in selecting case suitable for reporting. For instance, to ensure that the more serious cases are identified for reporting, criteria might refer to such indicators of systemic impact such as size of monetary settlements or awards. There is a need to report cases including significant or novel interpretations. There is also a value in reporting some typical cases which raise no novel legal issues but which illustrate the operation of the CBPR program in action.

Q. Why are case notes typically reported in anonymous form?

A. Case notes seek to illustrate the operation of the CBPR scheme, to educate about matters of interpretation and to ensure those handling complaints remain accountable. These objectives do not necessarily require the respondent to be named. The major objective of the complaints system is to resolve consumer disputes. Subject to the requirements of any particular scheme, this is often facilitated by confidential conciliation or mediation between the parties which does not require, and may even be hampered by, naming respondents publicly.

Q. Might it be useful to name respondents sometimes?

A. Sometimes it will be appropriate to name the respondent to a complaint. Indeed, some CBPR programs might have this as their usual practice. Even programs that do not usually name respondents may need to do so sometimes, for instance where the respondent has publicly announced that the program is handling the complaint or that fact has otherwise become a matter of public notoriety. Occasionally, naming a respondent is an intentional part of the complaint outcome (e.g. if the respondent is refusing to cooperate with the investigation or accept the outcome). It will be good practice for Accountability Agents to adopt transparent policies on their practices for naming respondents.

Q. How much detail should appear in the case notes?

A. When publishing case notes in anonymous form, care needs to be taken in publishing details which might inadvertently identify the parties. Anonymity is usually easily achieved through generalizing factual details. The level of useful detail in a particular case note will depend upon why it has been chosen for reporting. For example, complaints selected for a case note to illustrate a novel matter of legal interpretation will need the legal reasoning to be set out in full detail. By contrast, a case-note illustrating a fairly routine interpretation in an interesting factual-setting will obvious pay more attention to the facts. In the early phases of a scheme, relatively simple case notes are acceptable to ensure that advisers understand basic concepts but these should be followed by more detailed notes as familiarity with basic concepts is established.

Q. How should Accountability Agents disseminate case notes?

A. Active steps should be taken to make case notes easily available. Useful approaches may include to:

- maintain a distribution list to which copies of case notes are emailed
- release case notes individually or in batches during the year with accompanying media statements
- prepare summaries and use these in newsletters to highlight the release of new case notes
- post case notes on the Accountability Agent's website with good indexing and retrieval tools
- distribute electronic copies through RSS feeds
- integrate case notes into other educative initiatives such as training packages
- co-operate in re-publication by legal publishers.

Q. How can Accountability Agents assist in making case notes readily available throughout the Asia Pacific?

A. The cross-border nature of a CBPR program means that case notes will be useful to consumers, businesses, regulators and advisers in a variety of economies and not just in the Accountability Agent's home economy. Extra efforts should be taken to make their case notes widely available. These extra efforts will also contribute to consistency in interpretation across the region. Two key steps that Accountability Agents can take to make their case notes accessible throughout the Asia Pacific include:

- to facilitate the efforts of those who wish to re-publish their case notes
- to provide their case notes, in electronic form, to a recognised international consolidated point of access.

Q. How can Accountability Agents facilitate the efforts of those who wish to republish their case notes?

A. Third party publishers can enable case notes to be made more widely available to the public, specialist bodies, advisers, researchers and regulators. Accountability Agents may facilitate re-publication by giving a general license for re-publication of case notes with

proper acknowledgement. The general license should be included with the usual copyright statement posted on an Accountability Agent's website.

Q. Is there a place where all case notes could be deposited and accessed?

A. There is considerable value in having consolidated point of access for case notes from a variety of privacy enforcement authorities and accountability agents. The World Legal Information Institute's International Privacy Law Library available at www.worldlii.org/int/special/privacy provides a specialist facility for hosting privacy case notes and has for many years published case notes from privacy enforcement authorities in various Asia Pacific economies. The consolidated access point brings a variety of benefits including the ability to search seamlessly across a range of case note series from within the region. Accountability Agents are encouraged to make arrangements with WorldLII for the supply of case notes and their republication.

Q. *Is there any further published guidance on releasing case notes?*

A. The following resources discuss issues in releasing case notes and provide examples:

- International Privacy Law Library available at www.worldlii.org/int/special/privacy - which includes many examples of privacy case note series
- Graham Greenleaf, 'Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability for Asia-Pacific Privacy Commissioners', 2004 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=512782
- Asia-Pacific Privacy Authorities Statement of Common Administrative Practice on Case Note Citation, November 2005, available at www.privacy.gov.au/international/appa/statement.pdf
- Asia-Pacific Privacy Authorities Statement of Common Administrative Practice on Case Note Dissemination, November 2006, available at www.privacy.gov.au/international/appa/statement2.pdf
- OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, 2007, clause 20, available at www.oecd.org/dataoecd/43/28/38770483.pdf

Annex E

ACCOUNTABILITY AGENT COMPLAINT STATISTICS

The Accountability Agent recognition criteria require applicant Accountability Agents to attest that as part of their dispute resolution mechanism they have a process for releasing complaint statistics and for communicating that information to the relevant government agency and privacy enforcement authority.

The template, with associated guidance and FAQs will assist in meeting the requirement.

Objectives of Reporting Complaint Statistics

Complaints handling is an important element of the Cross-Border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the CBPR program;
- increase transparency across the CBPR system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the CBPR program across the APEC region; and
- promote accountability of those involved in complaints handling and build stakeholder trust in Accountability Agents.

Commentary on the Template

The template is provided as a tool for accountability agents. It is acceptable to depart from the template by reporting additional statistics. However, the core minimum statistics should be reported in each case since they will form a common and comparable minimum data set across all APEC Accountability Agent dispute resolution processes. In particular jurisdictions, governmental authorities may require the reporting of additional statistics.

Complaint numbers

The total number of complaints should be reported. Where no complaints are received, the complaint statistics template should be submitted indicating "none" to ensure it is clear that no complaints were received that year. A format for reporting will need to be adopted that makes clear the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. Some programs may treat all matters as complaints while others may reserve that term for more formal dispute resolution or investigation and have another category for the matters treated less formally.

Complaint outcomes

This part of the template provides a picture of the processing of complaints.

Complaints type

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the Accountability Agent is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

Complaints process quality measures

There statistics give a picture as to how well the complaints resolution system is working. At a minimum, some indication as to timeliness should be reported. At its simplest this might be to highlight the number or complaints that took longer than a target date to resolve (e.g. number of complaints on hand that are older than, say, three months) while some complaints systems may be able to produce a variety of more detailed statistics (e.g. the average time to resolve certain types of complaints). In a more sophisticated system other quality measures may be included and an Accountability Agent might, for example, report against internal targets or industry benchmarks if these are available.

General

The Accountability Agent should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

COMPLAINT STATISTICS TEMPLATE

Complaint Numbers
Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term 'complaint' is being used in the reported statistics.
Complaint Processing and Outcomes
Complaints processed during the year broken down by the outcome. Examples of typical outcomes include: • complaints that could not be handled as they were outside the program's jurisdiction (e.g. against a company that is not part of the CBPR program); • complaints referred back to a business that are resolved at that point; • complaints settled by the Accountability Agent; • complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority; • complaints for which the Accountability Agent has made a finding (such as complaint dismissed, complaint upheld in part, complaint upheld in full). When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action. The Accountability Agent should include a comment on the significance of the complaints outcomes.
Complaints Type
Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful

classifications will include:

- complaint subject matter broken down by APEC information privacy principle (notice, collection limitation, use, etc);
- basic information about complainants, where known, such as the economy from which complaints have been made;
- Information about the type of respondents to complaints – this will vary on the nature of a particularly CBPR program but may include industry classification (e.g. financial service activities, insurance), the capacity in which the respondent falls (e.g. information processor, employer, service provider), or size of company (SME, large company etc).

The Accountability Agent should comment on the significance of the reported figures.

Complaints Process Quality Measures

An indication should be given as to about any quality measures used in relation to the particular CBPR program. A typical measure may relate to timeliness. The Accountability Agent should offer a comment upon the figures reported.

COMPLAINT STATISTICS FREQUENTLY ASKED QUESTIONS

Q. *Why does APEC require complaint statistics to be released?*

A. Complaints statistics are part of a transparent and accountable complaints handling system. The statistics will help paint a picture of how the CBPR program is operating. A number of stakeholders have an interest in seeing such a picture. For example, companies within a CBPR program, consumer advocates and regulators all have interest in knowing what happens in relation to the processing of complaints through an Accountability Agent. Transparency will promote understanding and confidence in the system.

Q. *Why do I need to release statistics on all the topics in the template?*

A. The template lists a minimum set of statistics that should be reported. To get a complete picture, all the categories of statistics are needed. Furthermore, since these are standard requirements across all APEC economies, the resultant statistics should be reasonably comparable. Over time, a picture should emerge as to how well CBPR programs are working and whether change is desirable.

Q. *How should these statistics be presented?*

A. The template provides the statistics that should be reported and requires that the Accountability Agent comment upon the significance of the figures. It is recommended that the statistics reported for a particular period should be published alongside the equivalent statistics for previous recent periods. Where available, three or four year's worth of figures should be reported. Accountability Agents are encouraged to put some effort tin to clearly displaying and explaining the statistics so that stakeholders can better appreciate their significance. For example, clear tables of figures with accompanying graphs are helpful.

Q. *Are there steps that can be taken to facilitate comparison across APEC jurisdictions?*

A. Accountability Agents are to include a classification in their reported statistics based on the APEC information privacy principles. This will aid comparison. In classifying respondents to complaints by industry type, it is recommended that the International Standard Industrial Classification of All Economic Activities (revised by the United Nations in 2008) be used or national or regional standards on industry classification that are aligned with that international standard. (See http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27&Lg=1

Annex F

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party attests to the truth of the answers given.

_____ _____

[Signature of person who has authority to commit party to the agreement] **[Date]**

[Typed name]

[Typed title]

[Typed name of organization]

[Address of organization]

[Email address]

[Telephone number]

The first APEC recognition for an Accountability Agent is limited to one year from the date of recognition. Recognition for the same Accountability Agent will be for two years thereafter. One month prior to the end of the recognition period, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.

Asia-Pacific
Economic Cooperation

ACCOUNTABILITY AGENT APEC RECOGNITION APPLICATION
FOR THE PRP SYSTEM

OVERVIEW

The purpose of this document is to guide the application process for Accountability Agents seeking APEC recognition under the APEC Privacy Recognition for Processors (PRP) System. This document explains the necessary recognition criteria and provides the baseline program requirements of the PRP System. Only APEC-recognized Accountability Agents may participate in the PRP System. Once recognized, Accountability Agents may publicize this recognition and certify organizations as PRP-compliant.

APPLICATION PROCESS

In order to be considered eligible for recognition by APEC Economies, an Applicant Accountability Agent must:

- Explain how it is subject to the jurisdiction of the relevant enforcement authority in a PRP participating Economy[1]; *AND*
- Describe how each of the Accountability Agent Recognition Criteria (Annex A) have been met using the Accountability Agent Recognition Criteria Checklist (Annex B); *AND*
- Agree to make use of the template documentation developed and endorsed by APEC Economies (the PRP Intake Questionnaire, which includes questions to be answered by the applicant organization and baseline program requirements) against which the Accountability Agent would assess the applicant organization[2] when certifying organizations as PRP-compliant; *OR* demonstrate how their existing intake and review processes meet the baseline established using the PRP Program Requirements Map (Annex C); *AND*
- Complete the signature and contact information sheet (Annex F).

The completed signature and contact information sheet and all necessary supporting documentation should be submitted to the relevant government agencies or public authorities in any Economy in which the Applicant Accountability Agent intends to operate for an initial review to ensure the necessary documentation is included in the application, or other review as appropriate. The agency or authority may consult with other government agencies or authorities where necessary and will forward all information received to the Chair of the Electronic Commerce Steering Group, the Chair of the Data Privacy Subgroup and the Chair of the Joint Oversight Panel (JOP) where appropriate. The JOP will review the submitted information (and request any additional information that may be needed) when considering recommending the Applicant Accountability Agent for recognition by APEC Economies as an APEC PRP System Accountability Agent.

---

[1] An Economy is considered a participant in the Privacy Recognition for Processors System pursuant to the terms established in Paragraph 3.1 of the "Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel"

[2] Available at *https://cbprs.blob.core.windows.net/files/PRP%20-%20Intake%20Questionnaire.pdf*

Annex A

ACCOUNTABILITY AGENT RECOGNITION CRITERIA

CRITERIA

Conflicts of Interest

1) General Requirements:

   a. An Accountability Agent must be free of actual or potential conflicts of interest in order to participate in the APEC Privacy Recognition for Processors (PRP) System. For the purposes of participation as an Accountability Agent in the PRP System, this means the ability of the Accountability Agent to perform all tasks related to an Applicant organization's certification and ongoing participation in the PRP System free from influences that would compromise the Accountability Agent's professional judgment, objectivity and integrity.

   b. An Accountability Agent must satisfy the APEC member economies with evidence that internal structural and procedural safeguards are in place to address potential and actual conflicts of interest. Such safeguards should include but not be limited to:

      i. Written policies for disclosure of potential conflicts of interest and, where appropriate, withdrawal of the Accountability Agent from particular engagements. Such withdrawal will be required in cases where the Accountability Agent is related to the Applicant organization or Participant to the extent that it would give rise to a risk that the Accountability Agent's professional judgment, integrity, or objectivity could be influenced by the relationship.

      ii. Written policies governing the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.

      iii. Written policies for internal review of potential conflicts of interest with Applicant organizations and Participating organizations.

      iv. Published certification standards for Applicant organizations and Participating organizations (see paragraph 4 'Program Requirements').

      v. Mechanisms for regular reporting to the relevant government agency or public authority on certification of new Applicant organizations, audits of existing Participant organizations, and complaint processing.

      vi. Mechanisms for mandatory publication of case reports in certain circumstances.

2) Requirements with respect to particular Applicant organizations and/or Participant organizations

   a. At no time may an Accountability Agent have a direct or indirect affiliation with any Applicant organization or Participant organization that would prejudice the ability of the Accountability agent to render a fair decision with respect to their certification and ongoing participation in the PRP System, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during complaint processing and enforcement of the Program Requirements against a Participant. Such affiliations, which include but are not limited to the Applicant organization or Participant organization and the Accountability Agent being under common control such that the Applicant organization or Participant organization can exert undue influence in the Accountability Agent, constitute relationships that require withdrawal under 1(b)(i).

   b. For other types of affiliations that may be cured by the existence of structural safeguards or other procedures undertaken by the Accountability Agent, the existence of any such affiliations between the Accountability Agent and the Applicant organization or Participant organization must be disclosed promptly to the Joint Oversight Panel, together with an explanation of the safeguards in place to ensure that such affiliations do not compromise the Accountability Agent's ability to render a fair decision with respect to such an Applicant organization or Participant organization. Such affiliations include but are not limited to:

      i. officers of the Applicant organization or Participant organization serving on the Accountability Agent's board of directors in a voting capacity, and vice versa;

      ii. significant monetary arrangements or commercial relationship between the Accountability Agent and the Applicant organization or Participant organization, outside of the fee charged for certification and participation in the CBPR or PRP System; or

      iii. all other affiliations which might allow the Applicant organization or Participant organization to exert undue influence on the Accountability Agent regarding the Applicant organization's certification and participation in the PRP System.

   c. Outside of the functions described in paragraphs 5-14 of this document or those related to the CBPR certification of an Applicant or Participant, an Accountability Agent will refrain from performing for its Participants or Applicants services for a fee or any interest or benefit such as the following categories:

      i. consulting or technical services related to the development or implementation of Participant organization's or Applicant organization's data privacy practices and procedures;

ii. consulting or technical services related to the development of its privacy policy or statement; or

iii. consulting or technical services related to its security safeguards.

d. An Accountability Agent may be engaged to perform consulting or technical services for an Applicant organization or Participant organization other than services relating to their PRP and/or CBPR certification and on-going participation in the PRP and/or CBPR Systems. Where this occurs, the Accountability Agent will disclose to the Joint Oversight Panel:

i. the existence of the engagement; and

ii. an explanation of the safeguards in place to ensure that the Accountability Agent remains free of actual or potential conflicts of interest arising from the engagement [*such safeguards may include segregating the personnel providing the consulting or technical services from the personnel performing the functions described in paragraphs 5 -14 of this document and those related to the CBPR certification of an Applicant or Participant*].

e. Provision of services as required in Sections 3 through 6 shall not be considered performing consulting services which might trigger a prohibition contained in this document.

3) In addition to disclosing to the Joint Oversight Panel all withdrawals described above in Section 1(b)(i), an Accountability Agent also shall disclose to the Joint Oversight Panel those activities or business ventures identified in subsection 1(b) above that might on their face have been considered a conflict of interest but did not result in withdrawal. Such disclosures should include a description of the reasons for non- withdrawal and the measures the Accountability Agent took to avoid or cure any potential prejudicial results stemming from the actual or potential conflict of interest.

Program Requirements

4) An Accountability Agent evaluates Applicant organizations against a set of program requirements that encompass applicable principles of the APEC Privacy Framework with respect to processors and that meet the PRP System requirements developed and endorsed by APEC member economies (to be submitted along with this form, see Annex C). (*NOTE:* an Accountability Agent may charge a fee to a Participant for provision of these services without triggering the prohibitions contained in paragraph 1 or 2.)

Certification Process

5) An Accountability Agent has a comprehensive process to review an Applicant organization's policies and practices with respect to the Applicant organization's participation in the PRP System and to verify its compliance with the Accountability Agent's program requirements. The certification process includes:

    a) An initial assessment of compliance, which will include verifying the contents of the self-assessment forms completed by the Applicant organization against the program requirements for Accountability Agents, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

    b) A comprehensive report to the Applicant organization outlining the Accountability Agent's findings regarding the Applicant organization's level of compliance with the program requirements. Where non-fulfillment of any of the program requirements is found, the report must include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the PRP System.

    c) Verification that any changes required under subsection (b) have been properly completed by the Applicant organization.

    d) Certification that the Applicant organization is in compliance with the Accountability Agent's program requirements. An Applicant organization that has received such a certification will be referred to herein as a "Participant" in the PRP System.

On-going Monitoring and Compliance Review Processes

6) Accountability Agent has comprehensive written procedures designed to ensure the integrity of the Certification process and to monitor the Participant throughout the certification period to ensure compliance with the Accountability Agent's program.

7) In addition, where there are reasonable grounds for the Accountability Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. Where non-compliance with any of the program requirements is found, the Accountability Agent will notify the Participant outlining the corrections the Participant needs to make and a reasonable timeframe within which the corrections must be completed. The Accountability Agent must verify that the required changes have been properly completed by the Participant within the stated timeframe.

Re-Certification and Annual Attestation

8) Accountability Agent will require Participants to attest on an annual basis to the continuing adherence to the PRP program requirements. Regular comprehensive reviews will be carried out to ensure the integrity of the re-Certification. Where there has been a material change to the Participant's privacy policy (as reasonably determined by the Accountability Agent in good faith), an immediate review process will be carried out. This re-certification review process includes:

    a) An assessment of compliance, which will include verification of the contents of the self-assessment forms updated by the Participant, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools.

    b) A report to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification.

    c) Verification that required changes have been properly completed by Participant.

    d) Notice to the Participant that the Participant is in compliance with the Accountability Agent's program requirements and has been re-certified.

Complaint Processing Procedures

9) An Accountability Agent must have a mechanism to receive and process complaints about Participants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on complaint processing with other Accountability Agents recognized by APEC economies when appropriate and where possible. An Accountability Agent may choose not to directly supply the complaint processing mechanism. The complaint processing mechanism may be contracted out by an Accountability Agent to a third party. Where the complaint processing mechanism is contracted out by an Accountability Agent the relationship must be in place at the time the Accountability Agent is recognized under the APEC PRP System.

10) Complaint processing, whether supplied directly or by a third party under contract, includes the following elements:

    a) A process for receiving complaints both from individuals and personal information controllers and determining whether a complaint concerns the Participant's obligations under the program and that the complaint falls within the scope of the program's requirements.

    b) A process for notifying the complainant of the determination made under subpart (a), above.

c) Where the complaint is from an individual and concerns the processing of his/her personal information and the Participant's obligations under the program:

i. A timely process for forwarding the complaint either (i) to the Participant and verifying that the Participant has forwarded it to the controller where the applicable controller can be identified or, where obligated by the controller, handled it directly; or (ii) to the applicable controller for handling.

ii. Written notice by the Accountability Agent or contracted third party supplier of the complaint processing service to the complainant and the Participant when the complaint has been forwarded.

iii. A process for obtaining an individual's consent before sharing that individual's personal information with the relevant enforcement authority in connection with a request for assistance.

d) A process for making publicly available statistics on the types of complaints received by the Accountability Agent or its third party contractor and how such complaints were processed, and for communicating that information to the relevant government agency and privacy enforcement authority (see Annex D).

Mechanism for Enforcing Program Requirements

11) Accountability Agent has the authority to enforce its program requirements against Participants, either through contract or by law.

12) Accountability Agent has a process in place for notifying Participant immediately of non-compliance with Accountability Agent's program requirements and for requiring Participant to remedy the non-compliance within a specified time period.

13) Accountability Agent has processes in place to impose the following penalties, which are proportional to the harm or potential harm resulting from the violation, in cases where a Participant has not complied with the program requirements and has failed to remedy the non-compliance within a specified time period. [*NOTE*: In addition to the penalties listed below, Accountability Agent may execute contracts related to legal rights and, where applicable, those related intellectual property rights enforceable in a court of law.]

a) Requiring Participant to remedy the non-compliance within a specified time period, failing which the Accountability Agent shall remove the Participant from its program.

b) Temporarily suspending the Participant's right to display the Accountability Agent's seal.

c) Naming the Participant and publicizing the non-compliance.

d) Referring the violation to the relevant public authority or privacy enforcement authority. [*NOTE*: this should be reserved for circumstances

where a violation raises to the level of a violation of applicable law.]

e) Other penalties – including monetary penalties – as deemed appropriate by the Accountability Agent.

14) Accountability Agent will refer a matter to the appropriate public authority or enforcement agency for review and possible law enforcement action, where applicable, where the Accountability Agent has a reasonable belief pursuant to its established review process that a Participant's failure to comply with the APEC PRP System requirements has not been remedied within a reasonable time under the procedures established by the Accountability Agent pursuant to paragraph7 so long as such failure to comply can be reasonably believed to be a violation of applicable law.

15) Where possible, Accountability Agent will respond to requests from enforcement entities in APEC Economies that reasonably relate to that Economy and to the PPR-related activities of the Accountability Agent.

Annex B

ACCOUNTABILITY AGENT RECOGNITION CRITERIA CHECKLIST

Conflicts of Interest

1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.

2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.

3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

Program Requirements

4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

Certification Process

5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.

On-going Monitoring and Compliance Review Processes

6. Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).

7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

Re-Certification and Annual Attestation

8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

Complaint Processing

9. Applicant Accountability Agent should describe the mechanism to receive and process complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.

10. Applicant Accountability Agent should describe how the complaint processing meets the requirements identified in 10 (a) – (d) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party

supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

Mechanism for Enforcing Program Requirements

11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.

12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.

13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].

15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

Annex C

APEC PRIVACY RECOGNTION FOR PROCESSORS SYSTEM PROGRAM REQUIREMENTS MAP

SECURITY SAFEGUARDS

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (e.g. password protections) • Encryption • Boundary protection (e.g. firewalls, intrusion detection) • Audit logging • Monitoring (e.g. external and internal audits, vulnerability scans)	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
	• Other (specify) The Applicant must periodically review and reassess these measures to evaluate their relevance and effectiveness**.** Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	
3. Describe how your organization makes employees aware of the importance of maintaining the security of personal information.	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify)	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
	Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	
4. Has your organization implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures related to personal information**.** Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this principle.	
5. Does your organization have processes in place to test the effectiveness of the safeguards referred to in the question above? Please describe.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	
6. Do you have a process in place to notify the controller of occurrences of a breach of the privacy or security of their organization's	The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
personal information?	of the privacy or security of their organization's personal information.	
7. Has your organization implemented procedures for the secure disposal or return of personal information when instructed by the controller or upon termination of the relationship with the controller?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	
8. Does your organization use third-party certifications or other risk assessments? Please describe.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	

ACCOUNTABILITY MEASURES

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	The Accountability Agent must verify that the Applicant has policies in place to limit its processing to the purposes specified by the controller.	
10. Does your organization have procedures in place to delete, update, and correct information upon request from the controller?	The Accountability Agent must verify that the Applicant has measures in place to delete, update, and correct information upon request from the controller where necessary and appropriate.	
11. What measures does your organization take to ensure compliance with the controller's instructions related to the activities of personal information processing? Please describe.	The Accountability Agent must verify that the Applicant indicates the measures it takes to ensure compliance with the controller's instructions.	
12. Have you appointed an individual(s) to be responsible for your overall compliance with the requirements of the PRP?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with the PRP. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
	employee(s) is required for compliance with the PRP.	
13. Does your organization have procedures in place to forward privacy-related individual requests or complaints to the controller or to handle them when instructed by the controller?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to handle, or forward to the controller as appropriate, privacy-related complaints or requests. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	
14. Does your organization notify controllers, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place for notifying the controller, except where prohibited by law, of judicial or other government subpoenas, warrants or orders that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
	Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	
15. Does your organization have a procedure in place to notify the controller of your engagement of subprocessors?	The Accountability Agent must verify that the Applicant has in place a procedure to notify controllers that the Applicant is engaging subprocessors.	
16. Does your organization have mechanisms in place with subprocessors to ensure that personal information is processed in accordance with your obligations under the PRP? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such mechanisms is required for compliance with this principle.	
17. Do the mechanisms referred to above generally require that subprocessors:	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
a) Follow-instructions provided by your organization relating to the manner in which personal information must be handled? b) Impose restrictions on further subprocessing c) Have their PRP recognized by an APEC Accountability Agent in their jurisdiction? d) Provide your organization with self-assessments or other evidence of compliance with your instructions and/or agreements/contracts? If **YES**, describe. e) Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. f) Other (describe)		

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Relevant Program Requirement**
18. Do you have procedures in place for training employees pertaining to your privacy policies and procedures and related client instructions? Please describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this requirement.	

Annex D

ACCOUNTABILITY AGENT COMPLAINT STATISTICS

The Accountability Agent recognition criteria require applicant Accountability Agents to attest that as part of their complaint processing mechanism they have a process for releasing complaint statistics and for communicating that information to the relevant government agency and privacy enforcement authority.

The template, with associated guidance and FAQs will assist in meeting the requirement.

Objectives of Reporting Complaint Statistics

Complaints processing is an important element of the Privacy Recognition for Processors (PPR) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the PRP program;
- increase transparency across the PRP system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the PRP program across the APEC region; and
- promote accountability of those involved in complaints processing and build stakeholder trust in Accountability Agents.

Commentary on the Template

The template is provided as a tool for Accountability Agents. It is acceptable to depart from the template by reporting additional statistics. However, the core minimum statistics should be reported in each case since they will form a common and comparable minimum data set across all APEC Accountability Agent complaint processing. In particular jurisdictions, governmental authorities may require the reporting of additional statistics.

Complaint numbers

The total number of complaints should be reported. A format for reporting will need to be adopted that makes clear the number of new complaints received.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. Some programs may treat all matters as complaints while others may reserve that term for more formal complaints.

Complaint outcomes

This part of the template provides a picture of the processing of complaints.

Complaints type

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the Accountability Agent is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

Complaints process quality measures

These statistics give a picture as to how well the complaint processing system is working. At a minimum, some indication as to timeliness of complaint processing should be reported. At its simplest this might be to highlight the number or complaints that took longer than a target date to forward appropriately to the Participant or controller.

General

The Accountability Agent should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

COMPLAINT STATISTICS TEMPLATE

Complaint Numbers
Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term 'complaint' is being used in the reported statistics.
Complaint Processing and Outcomes
Complaints processed during the year broken down by the outcome. Examples of typical outcomes include: • complaints that could not be handled as they were outside the program's jurisdiction (e.g. against a company that is not part of the PRP program); • complaints forwarded to the Participant; • complaints forwarded to the applicable controller; • complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority, where applicable; When the Accountability Agent has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action. The Accountability Agent should include a comment on the significance of the complaints outcomes.
Complaints Type
Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful

Classifications will include:

- complaint subject matter broken down by APEC information privacy principle (security safeguards and accountability);
- basic information about complainants, where known, such as the economy from which complaints have been made.
- Information about the type of respondents to complaints – this will vary on the nature of a particularly PRP program but may include industry classification (e.g. financial service activities, insurance) or size of company (SME, large company etc).

The Accountability Agent should comment on the significance of the reported figures.

Complaints Process Quality Measures

An indication should be given about any quality measures used in relation to the particular PRP program. A typical measure may relate to timeliness. The Accountability Agent should offer a comment upon the figures reported.

COMPLAINT STATISTICS FREQUENTLY ASKED QUESTIONS

Q. *Why does APEC require complaint statistics to be released?*

A. Complaints statistics are part of a transparent and accountable complaints processing system. The statistics will help paint a picture of how the PRP program is operating. A number of stakeholders have an interest in seeing such a picture. For example, companies within a PRP program, consumer advocates and regulators all have interest in knowing what happens in relation to the processing of complaints through an Accountability Agent. Transparency will promote understanding and confidence in the system.

Q. *Why do I need to release statistics on all the topics in the template?*

A. The template lists a minimum set of statistics that should be reported. To get a complete picture, all the categories of statistics are needed. Furthermore, since these are standard requirements across all APEC economies, the resultant statistics should be reasonably comparable. Over time, a picture should emerge as to how well PRP programs are working and whether change is desirable.

Q. *How should these statistics be presented?*

A. The template provides the statistics that should be reported and requires that the Accountability Agent comment upon the significance of the figures. It is recommended that the statistics reported for a particular period should be published alongside the equivalent statistics for previous recent periods. Where available, three or four years' worth of figures should be reported. Accountability Agents are encouraged to put some effort into clearly displaying and explaining the statistics so that stakeholders can better appreciate their significance. For example, clear tables of figures with accompanying graphs are helpful.

Q. *Are there steps that can be taken to facilitate comparison across APEC jurisdictions?*

A. Accountability Agents are to include a classification in their reported statistics based on the APEC information privacy principles. This will aid comparison. In classifying respondents to complaints by industry type, it is recommended that the International Standard Industrial Classification of All Economic Activities (revised by the United Nations in 2008) be used or national or regional standards on industry classification that are aligned with that international standard. (See http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27&Lg=1

Annex E

SIGNATURE AND CONTACT INFORMATION

By signing this document, the signing party attests to the truth of the answers given.

_____ _____

[Signature of person who has authority to commit party to the agreement] **[Date]**

[Typed name]

[Typed title]

[Typed name of organization]

[Address of organization]

[Email address]

[Telephone number]

APEC recognition is limited to one year from the date of recognition. Each year one month prior to the anniversary of the date of recognition, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.