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. 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.

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.

DocuSigned by:
Avani M. Desai
7A37D238001A43F...

4/8/2020

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

[Typed name]
Avani Desai

[Typed title]
President

[Typed name of organization]
Schellman & Company, LLC

[Address of organization]
4010 W. Boyscout Blvd Suite 600 Tampa, FL 33607

[Email address]
avani.desai@schellman.com

[Telephone number]
866-254-0000

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.