TEMPLATE NOTICE OF INTENT TO PARTICIPATE IN THE APEC PRIVACY RECOGNITION FOR PROCESSORS SYSTEM

TO: *CHAIR*, APEC Electronic Commerce Steering Group
CC: *CHAIR*, APEC Data Privacy Subgroup
CC: *CHAIR*, APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel

LETTER OF INTENT TO PARTICIPATE IN THE APEC PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEM

I am writing this Letter of Intent to participate in the APEC PRP System pursuant to Paragraph 3.1 of the "Charter of the APEC Cross-Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel" (Charter) on behalf of [MEMBER ECONOMY].

[IF APPLICABLE,] I confirm that [NAME OF THE CPEA PARTICIPANT], a Privacy Enforcement Authority in [MEMBER ECONOMY], is a participant in the Cross Border Privacy Enforcement Arrangement (CPEA).

In addition, I confirm that [MEMBER ECONOMY] intends to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 7.2 of the Charter.

Please find the following information attached to this letter:

- A narrative description of the relevant domestic laws and regulations and administrative measures which may apply to any PRP certification-related activities of an Accountability Agent operating within [MEMBER ECONOMY's] jurisdiction and the enforcement authority associated with these laws and regulations (*Annex A*); AND

- A narrative explanation of oversight and enforcement mechanisms available to ensure the effective oversight of processors recognized under the PRP in [MEMBER ECONOMY] (*Annex B*) and a completed APEC Privacy Recognition for Processors Enforcement Map (*Annex C*).

Any enquiries regarding this letter should be directed to [RELEVANT CONTACT POINT].

Annex A

DOMESTIC LAWS AND REGULATIONS APPLICIABLE TO ACCOUNTABILITY AGENT ACTIVITIES

[NARRATIVE DESCRIPTION]

Annex B

OVERSIGHT AND ENFORCEMENT MECHANISMS APPLICABLE TO PRP-CERTIFIED PROCESSORS

[NARRATIVE DESCRIPTION]

Annex C

APEC PRIVACY RECOGNTION FOR PROCESSORS SYSTEM REQUIREMENTS: ENFORCEMENT MAP

As outlined in the Charter of the APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel (JOP), an APEC Member Economy is considered a Participant in the PRP System after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:

(i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate in the PRP System and in the event that the Economy has indicated that it would provide oversight and enforcement of compliance against the PRP program requirements through a domestic law or regulations enforced by a Privacy Enforcement Authority, confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC CPEA;

(ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 7.2 of the Charter of the APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems Joint Oversight Panel;

(iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the JOP, submits to the Chair of the ECSG an explanation of oversight and enforcement mechanisms available to ensure the effective oversight of processors recognized under the PRP in that Economy, even if direct government backstop enforcement is not applicable; and

(iv) The JOP submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.

The purpose of Annex C is to assist Economies and the JOP in fulfilling the requirements of items (iii) and (iv):

- *This document provides the baseline program requirements of the APEC Privacy Recognition for Processors (PRP) System in order to guide the Economy's explanation of how each requirement may be enforced in that Economy; and*
- *The information provided by the Economy will form the basis of the JOP's report.*

Column 1 lists the questions in the intake questionnaire to be answered by an applicant organization when seeking PRP certification. Column 2 lists the assessment criteria to be used by an APEC-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Economy's ECSG delegation or appropriate governmental representative when explaining the enforceability of an applicant organization's answers in Column 1.

SECURITY SAFEGUARDS

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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) • 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.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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) 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.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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 personal information?	The Accountability Agent must verify that the Applicant has in place appropriate processes to notify the controller of occurrences of a breach 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.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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*)**	**Enforceability (*to be answered by the Economy)***
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 employee(s) is required for compliance with the PRP.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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 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.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
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.	

Question (*to be answered by the Applicant Organization*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy)***
17. Do the mechanisms referred to above generally require that subprocessors: 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)	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*)**	**Enforceability (*to be answered by the Economy)***
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.	