GLOBAL PRIVACY RECOGNITION FOR PROCESSORS (PRP) SYSTEM PROGRAM REQUIREMENTS MAP

*The purpose of this document is to provide the baseline program requirements of the Global Privacy Recognition for Processors (PRP) System which operationalize the Global CBPR Privacy Principles ("**Privacy Principles**")[1], and assist Global CBPR Forum-recognized Accountability Agents in an Applicant Organization's compliance with the Global PRP System.*

These program requirements are replicated in the Global PRP System Intake Questionnaire to help Applicant Organizations assess their compliance.

Accountability Agents are responsible for receiving an Applicant Organization's completed Intake Questionnaire and supporting documentation, verifying an Applicant Organization's compliance with the requirements of the Global PRP System and, where appropriate, assisting the Applicant Organization in modifying its policies and practices to meet the requirements of the Global PRP System. The Accountability Agent will certify those Applicant Organizations deemed to have met the minimum criteria for participation provided herein, and will be responsible for monitoring the Certified Organizations' compliance with the Global PRP System based on these criteria.

[1] The Global CBPR Privacy Principles are described in the *Global CBPR Framework*, available at http://www.globalcbpr.org/documents/.

SECURITY SAFEGUARDS

Question *(to be answered by the Applicant Organization)*	**Assessment Criteria** *(to be verified by the Accountability Agent)*
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that the implementation of a written information security policy is required for compliance with this Privacy Principle.
2. Describe the physical, technical and administrative safeguards that implement your organization's information security policy.	Where the Applicant Organization 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 Organization must periodically review and reassess these measures to evaluate their relevance and effectiveness. Where the Applicant Organization indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant Organization that the implementation of such safeguards is required for compliance with this Privacy 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 Organization'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 Organization 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 Organization that the existence of such procedures is required for compliance with this Privacy 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 Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant that the existence of such measures is required for compliance with this Privacy 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 Organization 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 Organization 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 Organization answers **YES**, the Accountability Agent must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this Privacy 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 Organization 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 Organization 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)***
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 Organization 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 Organization 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 Organization 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 Global PRP System?	Where the Applicant Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has designated an employee(s) who is responsible for the Applicant Organization's overall compliance with the Global PRP System. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that designation of such an employee(s) is required for compliance with the Global PRP System.
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 Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such procedures is required for compliance with this Privacy 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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization 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 Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that such procedures are required for compliance with this Privacy 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 Organization has in place a procedure to notify controllers that the Applicant Organization 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 Global PRP System? Please describe.	Where the Applicant Organization answers **YES**, the Accountability Agent must verify the existence of each type of mechanism described. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that implementation of such mechanisms is required for compliance with this Privacy Principle.
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) Be Global PRP-certified by a Global CBPR Forum-recognized 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.	The Accountability Agent must verify that the Applicant Organization makes use of appropriate methods to ensure their obligations are met.

e) Allow your organization to carry out regular spot checking or other monitoring activities? If **YES**, describe. f) Other (describe)	
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 Organization answers **YES**, the Accountability Agent must verify that the Applicant Organization has procedures in place for training employees relating to personal information management and the controller's instructions. Where the Applicant Organization answers **NO**, the Accountability Agent must inform the Applicant Organization that the existence of such procedures is required for compliance with this Privacy Principle.