Annex C

GLOBAL PRIVACY RECOGNTION FOR PROCESSORS SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP[1]

*As outlined in Annex A of the Global CBPR Forum Terms of Reference, a jurisdiction interested in Membership ("**Applicant**") and intending to implement the Global CBPR and/or Global PRP System(s) should submit an explanation of how the Global CBPR and/or Global Privacy Recognition for Processors (PRP) System Program Requirements may be enforced in that jurisdiction.*

The purpose of this document is to assist Applicants in fulfilling the above-mentioned requirement. This document provides the Global PRP System Program Requirements to guide an Applicant's explanation of how each requirement may be enforced in its jurisdiction. The information provided by the Applicant will be considered in the Global CBPR Forum Membership Committee's recommendation on the application.

Column 1 lists the questions in the intake questionnaire to be answered by an Applicant Organization when seeking Global PRP certification. Column 2 lists the assessment criteria to be used by a Forum-recognized Accountability Agent when verifying the answers provided in Column 1. Column 3 is for use by the Applicant to explain the enforceability of an Applicant Organization's answers in Column 1. Additional documentation to assist in these explanations may be submitted as necessary.

Contents

SECURITY SAFEGUARDS 2

ACCOUNTABILITY MEASURES 5

[1] Annex C and the table that follows do not purport to provide a complete and comprehensive account of the FTC's privacy enforcement authority. They are not intended to be relied on as legal advice and should not be used as statements of law in the context of legal proceedings.

SECURITY SAFEGUARDS

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability**
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.	The FTC enforces Section 5 of the FTC Act, 15 U.S.C.§ 45, which prohibits **unfair** or **deceptive** acts or practices in or affecting commerce. An act or practice is **deceptive** if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service. An act or practice is **unfair** when it causes, or is likely to cause, substantial injury to consumers that (i) is not reasonably avoidable by consumers themselves; and (ii) is not outweighed by countervailing benefits to consumers or to competition. A company that is certified to the Global PRP System must publicly declare that it will comply with the Global PRP Program Requirements and must make these program requirements publicly accessible. If the company fails to comply with any of these program requirements, its public representation of compliance may constitute an unfair or deceptive act or practice subject to Section 5 enforcement.
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.	

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability**
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.	Various practices may violate Section 5 of the FTC Act, 15 U.S.C. § 45, and subject a company to an enforcement action. Such practices include, but are not limited to: • Making a public representation relating to the security safeguards requirements and failing to comply with the representation; • Displaying a seal, trustmark or other symbol, such as the Global PRP Certification Mark, on the company's website or on any other of its own publicly available documentation that indicates that it participates in the Global PRP System and thus complies with the security safeguards requirements and failing to comply; or • Causing the company's name to appear on a list of companies that are certified for participation in the Global PRP System (e.g., lists on the websites of participating government authorities, privacy enforcement
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.	

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability**
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.	authorities, Global CBPR Forum-recognized Accountability Agents, or on a Global CBPR Forum-related website specifically dedicated to the operation of Global PRP privacy certification) thereby indicating that it complies with the security safeguards requirements and failing to comply.
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)***	**Enforceability**
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.	The FTC enforces Section 5 of the FTC Act, 15 U.S.C.§ 45, which prohibits **unfair** or **deceptive** acts or practices in or affecting commerce. An act or practice is **deceptive** if it is likely to mislead a consumer acting reasonably under the circumstances and is likely to affect a consumer's conduct or decision regarding a product or service. An act or practice is **unfair** when it causes, or is likely to cause, substantial injury to consumers that (i) is not reasonably avoidable by consumers themselves; and (ii) is not outweighed by countervailing benefits to consumers or to competition. A company that is certified to the Global PRP System must publicly declare that it will comply with the Global PRP Program Requirements and must make these program requirements publicly accessible. If the company fails to comply with any of these program requirements, its public representation of compliance may constitute an unfair or deceptive act or
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.	

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability**
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.	practice subject to Section 5 enforcement. Various practices may violate Section 5 of the FTC Act, 15 U.S.C. § 45, and subject a company to an enforcement action. Such practices include, but are not limited to: • Making a public representation relating to the accountability measures requirements and failing to comply with the representation; • Displaying a seal, trustmark or other symbol, such as the Global PRP Certification Mark, on the company's website or on any other of its own publicly available documentation that indicates that it participates in the Global PRP System and thus complies with the accountability
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.	

Question ***(to be answered by the Applicant Organization)***	**Assessment Criteria** ***(to be verified by the Accountability Agent)***	**Enforceability**
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.	measures requirements and failing to comply; or • Causing the company's name to appear on a list of companies that are certified for participation in the Global PRP System (e.g., lists on the websites of participating government authorities, privacy enforcement authorities, Global CBPR Forum-recognized Accountability Agents, or on a Global CBPR Forum-related website specifically dedicated to the operation of Global PRP privacy certification) thereby indicating that it complies with the accountability measures requirements and failing to comply.
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?	The Accountability Agent must verify that the Applicant Organization 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**
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)		
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.	