National Programs

BBB National Programs

Vendor Privacy Program Requirements

Last Modified: January 21, 2021

BBB National Programs' Vendor Privacy Program ("VPP") is designed to help personal information processors ("processors") headquartered outside of the United States demonstrate their ability to assist personal information controllers ("controllers") in complying with relevant privacy obligations. This document sets forth the baseline requirements of the VPP against which BBB National Programs will assess a processor seeking certification ("Applicant"). To receive certification, the processor must meet this baseline set of requirements.

BBB National Programs

GENERAL INFORMATION

i. Name of the organization seeking certification ("Applicant"):
_____

ii. Country where Applicant is headquartered:
_____

iii. List of subsidiaries and/or affiliates to be covered by this certification, their location, and the relationship of each to Applicant:

Name of subsidiary or affiliate	Location of subsidiary or affiliate	Relationship of subsidiary to Applicant

iv. Applicant's contact point for BBB National Programs VPP:
Name: _____
Title: _____
Email: _____
Phone: _____

v. For what offering(s) or type(s) of processing service(s) are you applying for recognition?
_____

SECURITY SAFEGUARDS

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
1. Has your organization implemented an information security policy that covers personal information processed on behalf of a controller?	Where the Applicant answers **YES**, BBB National Programs must verify the existence of this written policy. Where the Applicant answers **NO**, BBB National Programs 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, BBB National Programs 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)

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
	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, BBB National Programs 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.	BBB National Programs 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: o Regular staff meetings or other communications o Security policy signed by employees o Other (specify)

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by BBB National Programs*)
	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, BBB National Programs 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**, BBB National Programs 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**, BBB National Programs 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.	BBB National Programs 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.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
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?	BBB National Programs 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**, BBB National Programs must verify the existence of procedures for the secure disposal or return of personal information. Where the Applicant answers **NO**, BBB National Programs 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.	BBB National Programs 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, BBB National Programs must verify whether recommendations made in the audits are implemented.

ACCOUNTABILITY MEASURES

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
9. Does your organization limit its processing of personal information to the purposes specified by the controller?	BBB National Programs 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?	BBB National Programs 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.	BBB National Programs 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 Vendor Privacy Program?	Where the Applicant answers **YES,** BBB National Programs must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with the Vendor Privacy Program.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
	Where the Applicant answers **NO**, BBB National Programs must inform the Applicant that designation of such an employee(s) is required for compliance with the Vendor Privacy Program.
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,** BBB National Programs 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**, BBB National Programs 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?	**YES,** BBB National Programs 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.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by BBB National Programs*)
	Where the Applicant answers **NO**, BBB National Programs 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 sub-processors?	BBB National Programs 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 sub-processors to ensure that personal information is processed in accordance with your obligations under the Vendor Privacy Program? Please describe.	Where the Applicant answers **YES,** BBB National Programs must verify the existence of each type of mechanism described. Where the Applicant answers **NO**, BBB National Programs 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 sub-processors:	BBB National Programs must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
a) Follow-instructions provided by your organization relating to the manner in which personal information must be handled? b) Impose restrictions on further sub-processing? c) Have a certification that meets or exceeds the requirements of BBB National Programs' Vendor Privacy Program? 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?	Where the Applicant answers **YES**, BBB National Programs must verify that the Applicant has procedures in place for training employees relating to personal

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by BBB National Programs*)**
Please describe.	information management and the controller's instructions. Where the Applicant answers **NO**, BBB National Programs must inform the Applicant that the existence of such procedures is required for compliance with this requirement.