+1-617-398-7067
info@verasafe.com
www.verasafe.com

VIA EMAIL

July 3, 2025

Shannon Coe, Director, Global Data Policy
International Trade Administration
United States Department of Commerce
1401 Constitution Avenue N.W.
Room 4324
Washington, D.C. 20230

RE: Submission of Accountability Agent Application for the Global CBPR and PRP Systems: VeraSafe

Dear Ms. Coe:

Please accept this initial application by VeraSafe, LLC (**VeraSafe**), a Delaware limited liability company, to serve as an Accountability Agent for the for the Asia Pacific Economic Cooperation's (**APEC**) Global Cross Border Privacy Rules (**CBPR**) and Privacy Recognition for Processors (**PRP**) Systems (each, a **System**).

VeraSafe provides a comprehensive range of privacy, information security, and legal consulting services, including but not limited to proprietary privacy program certifications, penetration testing, General Data Protection Regulation compliance advising, dispute resolution services for the EU-U.S., UK Extension to the EU-U.S., and Swiss-U.S. Data Privacy Frameworks, Data Protection Representative services, Data Protection Officer services, and outside compliance review services in support of the Data Privacy Frameworks. Our Professional Services Department, with a team of professionals throughout the United States and internationally, provides our extensive data protection compliance and audit-related services.

The United States of America is an active participant in the APEC CBPR and PRP systems and has designated the Federal Trade Commission (**FTC**) as its regulatory enforcement authority. As a U.S.-based for-profit business entity, VeraSafe is subject to the direct regulatory oversight and enforcement authority of the FTC.

In the following pages, we describe how VeraSafe proposes to meet each of the Recognition Criteria as developed and approved by the APEC member economies (for the APEC CBPR and PRP Systems). Documentation and evidence to support the responses are provided in the appendices.

+1-617-398-7067
info@verasafe.com
www.verasafe.com

Should you have any questions about this application, please feel free to contact our Research and Services Development Division, at rsd@verasafe.com.

Best regards,

Matthew Joseph
President and Managing Director
VeraSafe

+1-617-398-7067
info@verasafe.com
www.verasafe.com

Index of Appendices

The appendices listed below are attached at the end of this document in support of the responses in the CBRP and PRP Systems Accountability Agent Recognition Criteria Checklists[1]:

Appendix A - VeraSafe Conflicts of Interest Policy and Procedures for the CBPR and PRP Systems (Business Proprietary and Confidential - Attached with Submission)

Appendix B - VeraSafe CBPR and PRP Systems Dispute Resolution Procedure (Attached with Submission)

Appendix C - VeraSafe APEC CBPR Forum Certification Program Addendum (Business Proprietary and Confidential - Attached with Submission)

[1] Available at https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-AccountabilityAgentApplication.pdf,https://cbprs.org/wp-content/uploads/2022/07/Accountability-Agent-Application-for-PRP-Revised-For-Posting-3-16.pdf (Last consulted on June 24, 2025)

+1-617-398-7067
info@verasafe.com
www.verasafe.com

CBPR/PRP Systems Accountability Agent Recognition Criteria Checklist

Conflicts of Interest

1. Applicant Accountability Agent should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.

Reputation, Certifications, Ethics, and Bar Rules

VeraSafe, LLC (**VeraSafe**) has built a reputation of excellence in the data privacy and data protection field since its founding in 2010. Central to maintaining this strong reputation is our commitment to objectivity, ethical integrity, and remaining free from conflicts of interest—or even the perception of such conflicts. This dedication is reflected not only in the high ethical standards upheld by our team but also in the professional services we provide. Through its Professional Services Department, VeraSafe delivers compliance and audit-related services with a focus on impartiality and rigor. These services are performed by a highly credentialed team, many of whom hold advanced industry-recognized certifications and designations, such as Certified Information Privacy Professional (CIPP), Artificial Intelligence Governance Professional (AIGP), Fellow of Information Privacy (FIP), Certified Information Privacy Manager (CIPM), Certified Information Privacy Technologist (CIPT), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Project Management Professional (PMP), Certified Ethical Hacker (CEH), Certified Chief Information Security Officer (CISO), and Certified Information Systems Security Professional (CISSP). In addition, some staff members contribute to industry advancements through roles such as members of the European Data Protection Board's Support Pool of Experts and the International Association of Privacy Professionals CIPP/US Examination Development Advisory Board.

Moreover, numerous staff members, particularly those holding titles such as Privacy Counsel, Senior Privacy Counsel, or Associate Privacy Counsel, are qualified attorneys within their jurisdictions. As such, they are bound to uphold the ethical standards and rules of conduct required by their respective bar associations, ensuring that their professional responsibilities at VeraSafe align with these rigorous standards of legal and ethical integrity. Through these affiliations and to maintain required credentials, VeraSafe staff must adhere to strict codes of ethics, objectivity, and integrity when performing assessment services.

Company-Wide Rules on Conflicts of Interest

To reinforce these standards, Section 31 of VeraSafe's Team Member Manual, which applies to all staff members, outlines the potential for conflicts of interest in a collaborative environment like VeraSafe. The manual states:

> *One of the most difficult aspects of legal practice in an association such as VeraSafe, where the knowledge of one lawyer may be imputed to others, is the risk of conflicts of interest. This concern includes the possibility not only of representing conflicting interests among VeraSafe clients in violation of applicable bar rules but also the undermining of clients' confidence in VeraSafe's ability to provide them competent representation. These rules are particularly stringent in the United States and the risk to VeraSafe as a U.S.-based company is significant.*
>
> *Because conflicts of interest are not always obvious and often do not arise until an engagement is already underway, all VeraSafe personnel must stay alert to and seek to minimize their potential. Keep in mind that conflicts specific to you will generally be imputed to every other VeraSafe team member. For this reason, while you are generally free to participate as an individual in community and political activities, no VeraSafe team member is permitted to provide legal advice or perform other work outside of their work for VeraSafe without the written consent of VeraSafe's President.*

Additionally, the Section outlines a clear procedure for internally reporting and addressing potential conflicts of interest.

Trademark Enforcement and FTC Enforcement

VeraSafe is fully committed to upholding the standards of the CBPR and PRP Systems, and upon approval of this application, will only issue its (forthcoming) certification marks to organizations that have demonstrated full compliance with all requirements. Authorizing the use of VeraSafe CBPR or PRP certification mark to an organization that does not meet all certification program requirements could expose VeraSafe to potential claims by the Federal Trade Commission (FTC) under Section 5(a) of the Federal Trade Commission Act (FTC Act) (15 U.S.C. § 45), which addresses "unfair or deceptive acts or practices in or affecting commerce." If approved as a CBPR and PRP Accountability Agent, VeraSafe would also take additional actions to support the integrity of the programs. For example, if we became aware that a foreign organization was improperly using our certification mark or a certification mark issued by the Global CBPR Forum, we would notify relevant regulators.

Conflicts of Interest Policy and Procedures for the CBPR and PRP Systems

VeraSafe has adopted the Conflicts of Interest Policy and Procedures for the CBPR and PRP Systems attached hereto as Appendix A (the **Conflicts Policy**), which includes internal structural and procedural safeguards to address potential and actual conflicts of interest and to ensure that we are

able to perform all tasks related to the certification and ongoing participation of an applicant or participant organization in the CBPR or PRP programs, free from influences that would compromise VeraSafe's professional judgment, objectivity, and integrity.

Our Conflicts Policy addresses requirements 1(a) and (b) of Annex A in the following ways:

1. **Prohibits Certain Affiliations.** The Conflicts Policy prohibits direct or indirect affiliation with any Applicant or Participant that would prejudice the ability of VeraSafe as an Accountability Agent to render a fair decision with respect to their certification and ongoing participation in a System, free from influences that would compromise its professional judgment, objectivity, and integrity, including but not limited to during the application review and initial certification process; during ongoing monitoring and compliance review; during re-certification and annual attestation; and during dispute resolution and enforcement of the Program Requirements against a Participant.

2. **Requires Withdrawal in Certain Situations.** The Conflicts Policy requires VeraSafe to withdraw from performing any certification or ongoing participation activities for an applicant or participant that would create, or appear to create, a significant risk of compromising VeraSafe's professional judgment, integrity, or objectivity.

3. **Requires Separation of Personnel.** The Conflicts Policy requires the separation of personnel handling privacy certification functions from personnel handling sales and consulting functions.

4. **Requires Internal Review for Conflicts of Interest.** The Conflicts Policy requires internal review for potential or actual conflicts between VeraSafe and any current or prospective applicant or participant.

2. Applicant Accountability Agent should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.

Our Conflicts Policy:

1. **Prohibits our Provision of Consulting or Technical Services Other Than Certification Services for an Applicant or Participant Except in Certain Situations.** The Conflicts Policy requires that before signing any non-Certification-related service agreement with an applicant or participant, and before signing a Certification-related agreement with an organization that receives or received consulting or technical services other than certification services, VeraSafe will (i) review the relationship for potential conflicts of interest, and (ii) disclose the non-Certification-related engagement to the Joint Oversight Panel (JOP) or the Global Forum Assembly (GFA), as applicable. If the JOP or the GFA object to the engagement after full disclosure, VeraSafe and the

applicant or participant will determine whether to proceed with either the Certification Services or the Non-Certification engagement, ensuring compliance with the Conflicts Policy.

2. **Requires Separation of Sales and Consulting Team Members from Team Members Providing Certification Services.** The Conflicts Policy requires that any VeraSafe staff member who was either (i) materially involved in selling or negotiating VeraSafe's Certification services, or (ii) materially involved in providing consulting or Data Protection Officer services, for an applicant or participant, shall not provide or otherwise be involved in the Certification services for such applicant or participant.

3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

Our Conflicts Policy:

1. **Requires Disclosure of Cured Potential Conflicts to the JOP or the GFA.** The Conflicts Policy requires that any potential conflicts of interest that have been cured through the implementation of appropriate safeguards and mechanisms must be disclosed to the JOP or the GFA.

2. **Requires Withdrawal from any Engagements Involving Conflicts of Interest.** The Conflicts Policy requires that any prohibited affiliation must not be engaged, and any such engagement must be withdrawn. For potential conflicts of Interest, VeraSafe will assess whether appropriate safeguards can be implemented to mitigate the risk. If a potential conflict cannot be mitigated through structural safeguards, VeraSafe will withdraw from the engagement.

3. **Requires Disclosure of Withdrawn Engagements to the JOP.** The Conflicts Policy requires that any engagements that have been withdrawn due to conflicts of interest, including (i) prohibited affiliations, or (ii) potential conflicts of interest that cannot be cured, must be disclosed to the JOP.

Program Requirements

4. Applicant Accountability Agent should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

Upon approval of this application, VeraSafe will make use of the APEC CBPR and PRP Program Requirements, posted at http://cbprs.org/documents, or the Global CBPR-forum CBPR and PRP Program Requirements, posted at https://www.globalcbpr.org/documents/, as applicable.

Certification Process

5. Applicant Accountability Agent should submit a description of how the requirements identified in 5(a)-(d) of Annex A have been met.

Upon approval of this application, VeraSafe will commence offering these services, which will commence with an initial assessment of compliance for each applicant organization. This process will include verifying the contents of the self-assessment forms completed by the applicant organization against the relevant program requirements, using the approved CBPR and PRP Intake Questionnaires and associated program requirements.

Upon an applicant organization's completion of the intake forms, VeraSafe will document the organization's compliance with each of the associated program requirements and provide a comprehensive report to the organization outlining its findings. If noncompliance with any program requirement is found, VeraSafe will communicate the required changes to the applicant organization for the applicant organization to obtain CBPR and/or PRP certification, as applicable, and review any corresponding changes to the applicant organization's policies and procedures. VeraSafe will then verify whether such changes have been properly completed by the applicant organization.

If VeraSafe determines that the applicant organization meets the program requirements for certification under the CBPR or PRP programs, as applicable, the applicant organization will be awarded a certification mark identifying their participation in the applicable program(s), to be displayed on the privacy notices within the scope of the certification. When a consumer clicks on this certification mark the consumer will be brought to a confirmation page that states (i) whether the organization is in good standing in the program, (ii) the scope of the organization's participation, and (iii) instructions on how to file a complaint concerning the organization using VeraSafe's Dispute Resolution Procedure (appended hereto as Appendix B). Once a certification has been awarded, the applicant organization will be referred to herein as a "Participant" in the CBPR and/or PRP Systems.

VeraSafe will then provide the relevant details of the Participant's certification for the CBPR and/or PRP compliance directories to APEC or the Global CBPR Forum through the established channels for the Systems, as applicable. The information shared will include:

- the name of the Participant;
- the URL of the Participant's website;
- the URL of the webpage where the Participant's privacy statement can be found;
- the name and email address of the Participant's appointed contact;
- the name of the Accountability Agent;
- the relevant Privacy Enforcement Authority(ies);

- the scope of the Participant's certification;
- the Participant's original certification date; and
- the date that the Participant's current certification expires.

Ongoing Monitoring and Compliance Review Processes

6. Applicant Accountability Agent should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the requirements described in 5(a)-(d).

Participants will be monitored throughout the certification process to ensure ongoing compliance with the CBPR and/or PRP programs in the following ways:

- **Self-reporting**. All Participants will be contractually required to notify VeraSafe of any changes to the policies and practices within the scope of the CBPR and/or PRP programs prior to the implementation of such changes for review against the relevant program requirements.
- **Website Change Monitoring**. All reviewed and approved privacy notices within the scope of a CBPR or PRP certification will be monitored to detect and track changes.
- **Third-party Reporting**. VeraSafe will investigate complaints against Participants that it receives through its Dispute Resolution Procedure.

If, through any of these methods, VeraSafe discovers reasonable grounds to believe that a Participant has engaged in a practice that may constitute a breach of the relevant program requirements, an immediate review process will be conducted. This review process will begin with an initial assessment within five business days of identifying the potential issue and additional steps that will take place over the course of thirty-five business days.

7. Applicant Accountability Agent should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

The scope of a review of a Participant will depend on specific circumstances surrounding the potential breach of the program requirement(s). If, through this review, VeraSafe identifies an actual breach of one or more program requirements, the participant will be sent a warning letter, which may be delivered via email, including a reasonable time frame within which the corrections must be completed, as per the Program Addendum (as defined below). This reasonable cure period generally

lasts twenty business days but may be extended for up to six months in more complex cases.[2] If the Participant fails to correct the identified non-compliance within this period, they will be suspended from the program. During such suspension, the use of the VeraSafe's certification mark will be revoked and the applicable compliance directories will be updated to reflect that the Participant is no longer active in the program.

Re-Certification and Annual Attestation

8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8(a)-(d) of Annex A.

To maintain good standing in the CBPR and/or PRP programs, a Participant must complete VeraSafe's recertification process within 12 months of such Participant's previous certification date. This re-certification mirrors the process described above. If the Participant proposes to make changes to their personal data processing and management practices at this time, those practices will be evaluated against the relevant program requirements to ensure that full compliance with the relevant program is maintained. If during this process, VeraSafe discovers any previously unreported non-compliance, the non-compliant practice will be treated as a breach of the program requirements, triggering the cure timeline described above. Failure to cure within that time will likewise result in a suspension.

Dispute Resolution Process

9. Applicant Accountability Agent should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents/other Accountability Agents that may be used when appropriate.

Find VeraSafe CBPR and PRP Systems Dispute Resolution Procedure ("**Dispute Resolution Procedure**") in Appendix B. By way of summary, VeraSafe will receive complaints through a secure webform and dedicated email inbox, as outlined in Section 5.3 of the Dispute Resolution Procedure.

[2] VeraSafe will assess complexity based on factors such as the scope and severity of the non-compliance, the number of systems or vendors/third parties involved, the complexity of data flows, and the presence of external dependencies beyond the Participant's control. While VeraSafe would allow for a cure period of up to six months in complex cases, VeraSafe recognizes that, in the context of a one-year certification cycle, such an extended period may be impractical. Accordingly, a six-month extension would only be granted in exceptional circumstances where the delay is both justified and compatible with the certification and re-certification timeline.

Upon receipt, each complaint will be evaluated for eligibility per Section 6.2, including whether it falls within the scope of the CBPR or PRP System obligations and whether the respondent is an active Participant in good standing.

VeraSafe will notify the Complainant of its eligibility determination (Sections 5.4 and 6.4), and if eligible, the Participant is required to respond within twenty business days (Section 7.1). VeraSafe may conduct an impartial investigation (Section 7.3), which includes reviewing submissions, interviewing relevant parties, and requesting clarifications.

All complaint handling is confidential and timely (Section 5.5), with a target resolution period of ninety calendar days.

If informal mediation fails, a formal Procedure Hearing may be initiated (Section 8), resulting in non-binding corrective measures outlined in a Reparation Order (Section 8.5 (b)(1)).

VeraSafe has established a mechanism to cooperate with other recognized Accountability Agents, as detailed in Section 6.6 and Section 11.4 of its Dispute Resolution Procedure. When a complaint implicates entities or participants outside the U.S. or requires interpretation across economies, VeraSafe will coordinate with other recognized Accountability Agents. This includes sharing information as appropriate, determining which agent is best placed to lead the complaint process, and collaborating on outcomes to ensure consistency and fairness.

VeraSafe will also maintain communication channels to support such cross-border collaboration in alignment with the CBPR and PRP interoperability expectations.

10. Applicant Accountability Agent should describe how the dispute resolution process meets the requirements identified in 10(a)-(h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E/Annexes E and F.

VeraSafe's dispute resolution process will be administered directly by VeraSafe, LLC and is described in full in the "VeraSafe CBPR and PRP Systems Dispute Resolution Procedure." The process meets the requirements of Annex A, Section 10(a)–(h) as follows:

a) Process for Receiving Complaints and Determining Scope

VeraSafe will receive complaints through its secure online form or via a designated email address (Section 5.3 of the Procedure). Each complaint will be assessed to determine whether it alleges non-compliance with the applicable CBPR or PRP System Requirements and whether it falls within the scope of the program (Section 6.2).

b) Notifying the Complainant of the Determination

VeraSafe will notify the complainant of its eligibility determination promptly after review (Sections 5.4 and 6.4). If the complaint is found ineligible, reasons will be provided. If additional information is needed, the complainant is contacted (Section 6.4).

c) Process for Investigating Complaints

Upon finding a complaint eligible, VeraSafe will investigate the facts and circumstances by reviewing documentation, requesting clarifications, and conducting interviews (Section 7.3). This investigation supports either informal resolution or a formal hearing process.

d) Timely and Confidential Resolution, Corrective Actions, and Deadlines

VeraSafe will process complaints in a timely and confidential manner (Sections 5.5 and 13.1). The goal is to resolve complaints within ninety calendar days from eligibility determination. Where non-compliance is found, VeraSafe will issue a written decision (Reparation Order) detailing corrective actions and a reasonable deadline for remediation (Section 8.5).

e) Written Notice of Resolution

VeraSafe will notify both the complainant and the participant of the outcome in writing, whether the complaint is resolved by mediation, settlement, or formal hearing (Sections 8.5 and 10.1).

f) Consent Before Sharing with Enforcement Authority

VeraSafe will obtain explicit consent from the complainant before sharing any personal information with relevant enforcement authorities (Sections 5.2 and 6.7).

g) Public Statistics and Communication to Authorities (Annex E)

VeraSafe will publish annual reports summarizing the number and types of complaints received, outcomes, resolution timelines, and referrals to authorities, unless none of the foregoing occurred during the relevant period. These reports will be anonymized where appropriate and communicated to the relevant privacy enforcement authority and government agencies (Section 12.1). This satisfies the requirements of **Annex E**.

h) Case Notes (Annex D)

Each Annual Procedure Report will include anonymized case notes on selected resolved complaints to illustrate typical or significant interpretations and outcomes (Section 12.1). These case notes fulfill the requirements of **Annex D**.

Conflict of Interest Statement

VeraSafe plans to deliver its dispute resolution services directly and does not plan to use third-party suppliers for complaint resolution. Therefore, the conflict-of-interest provisions in Annex A Sections 1–3 are addressed through VeraSafe's internal governance, which includes firewalling between certification services and complaint resolution, ensuring impartiality of Hearing Officers (Section 8.2(b)), and not permitting business interests to interfere with case handling.

Mechanism for Enforcing Program Requirements

11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants/Certified Organizations.

VeraSafe will require all applicant organizations to sign the VeraSafe APEC CBPR Forum Certification Program Addendum, (the "**Program Addendum**") detailing the terms of participation in the CBPR and/or PRP programs (see Appendix C).

Section 3.1(c) of the Program Addendum states "Notwithstanding the foregoing, if VeraSafe becomes aware of Participant's ongoing noncompliance with Program requirements then: (i) VeraSafe will notify Participant with particularity and detail; (ii) VeraSafe will specify (x) a reasonable cure period by which Participant must remedy the noncompliance and (y) penalties that may be imposed by VeraSafe if Participant fails to remedy the noncompliance (it being understood such penalties may include placing Participant on suspension with respect to its participation in the Program; reporting Participant's non-compliance to the U.S. Department of Commerce, U.S. Federal Trade Commission, or other appropriate government agencies; or other reasonable penalties proportional to the harm or potential harm resulting from the noncompliance); and (iii) upon Participant's reasonable request, VeraSafe will assist Participant in remedying the noncompliance."

Section 3.2(b) of the Program Addendum states "Upon VeraSafe's certification of Participant as compliant with the System, VeraSafe may grant Participant a revocable (in VeraSafe's sole discretion), non-exclusive, non-transferable, non-sublicensable, worldwide license to display VeraSafe's System-specific trust seal as reasonably directed by VeraSafe; provided that this license grant will automatically expire on the earliest to occur of (i) the end of the Program Term, (ii) the date on which Participant becomes due for its next annual assessment hereunder, and (iii) the date on which Participant loses its certification under the System for any other reason."

12. Applicant Accountability Agent should describe the policies and procedures for notifying a participant of non-compliance with Applicant's Program Requirements and provide a description of the processes in place to ensure the participant/Certified Organization remedies the non-compliance.

Section 3.1(c) of the Program Addendum states "[I]f VeraSafe becomes aware of Participant's ongoing noncompliance with Program requirements then:

(i) VeraSafe will notify Participant with particularity and detail;

(ii) VeraSafe will specify (x) a reasonable cure period by which Participant must remedy the noncompliance and (y) penalties that may be imposed by VeraSafe if Participant fails to remedy the noncompliance (it being understood such penalties may include placing Participant on suspension with respect to its participation in the Program; reporting Participant's non-compliance to the U.S. Department of Commerce, U.S. Federal Trade Commission, or other appropriate government agencies; or other reasonable penalties proportional to the harm or potential harm resulting from the noncompliance); and

(iii) upon Participant's reasonable request, VeraSafe will assist Participant in remedying the noncompliance."

In practice, the notification referred to in Section 3.1(c) of the Program Addendum shall take place within 1-2 business days of identifying the issue.

13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13(a)-(e) of Annex A.

To impose penalties for noncompliance with Program requirements, VeraSafe will follow a structured procedure to ensure fairness and proportionality. Once the cure period has expired without the Participant remedying the issue, VeraSafe will assess the severity and potential harm of the noncompliance. This assessment will consider factors such as:

- The nature and scope of the violation, including whether it involves a material breach of the relevant program requirements.
- The potential or actual impact on data subjects and regulatory compliance.
- Whether the Participant has previously been cited for similar or related issues.
- The Participant's cooperation in addressing the issue and history of compliance with program standards.

Based on this assessment, VeraSafe may impose one or more of the penalties as set forth in Section 3.1(c) of the Program Addendum, which expressly references suspension from the Program, notification to relevant regulatory authorities, or other reasonable penalties proportional to the harm or potential harm resulting from the noncompliance. These measures may include, but are not limited to:

- **Formal Reprimand:** Issuance of a formal warning detailing the violation and corrective actions required.
- **Temporary Suspension:** The Participant may be suspended from the program, during which time it must cease using VeraSafe's certification mark and will be flagged as inactive with respect to the certification program in compliance directories.
- **Public Disclosure of Noncompliance:** VeraSafe may publicly disclose the Participant's noncompliance in accordance with program guidelines.

- **Notification to Regulatory Authorities:** In cases involving significant or willful violations, VeraSafe may report the noncompliance to appropriate regulatory bodies.
- **Program Expulsion:** If noncompliance is severe, ongoing, or indicative of a fundamental inability to meet program requirements, the Participant may be permanently removed from the program.

VeraSafe will notify the Participant in writing of the penalty imposed, the rationale behind the decision, and any actions required to regain good standing, if applicable. Participants will have an opportunity to appeal certain penalties within a specified timeframe, providing additional information or remediation plans for reconsideration. Appeals will be reviewed by an internal VeraSafe compliance panel, which may uphold, modify, or overturn the penalty based on the evidence provided.

If a penalty requires corrective actions, VeraSafe will conduct a follow-up review to verify compliance. Participants who have been reinstated after a suspension or reprimand may be subject to increased monitoring for a defined period.

14. Applicant Accountability Agent should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action / the appropriate PEA(s) and relevant government entities for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances.]

General Referral Policies

Where required by law, regulatory agreements, or program rules, VeraSafe will report the following cases to the appropriate public authority or enforcement agency for review and possible law enforcement action:

- Violations of consumer protection, data protection, or privacy laws that fall under the jurisdiction of regulatory bodies such as the U.S. FTC or the U.S. Department of Commerce.
- Breaches that trigger mandatory reporting requirements under applicable regulations (e.g., failure to comply with a legally binding consent order).
- Situations where VeraSafe is explicitly required to notify enforcement authorities as part of its role as an Accountability Agent.

VeraSafe will provide additional information to public authorities upon request, while ensuring compliance with applicable confidentiality and data protection obligations.

Any formal actions taken by an enforcement agency in respect of the foregoing, to the extent VeraSafe is made aware of them, will be tracked and recorded in VeraSafe's compliance records.

Additionally, all referrals will be included in VeraSafe's Annual Procedure Report, providing transparency regarding enforcement measures and referral activities.

To ensure fairness and due process, VeraSafe will notify the Participant of a pending referral, except where legally prohibited or where immediate referral is required due to severity.

Referral in the Context of the Dispute Resolution Procedure

Sections 3.3(a)–(b) of the Program Addendum state that Participant is bound by and will cooperate with the VeraSafe Dispute Resolution Procedure, which may be updated from time to time.

Sections 11.1–11.3 of the Dispute Resolution Procedure state:

11. Referral To Government Agencies and Cooperation with Other Accountability Agents.
11.1*. Subject to Section 11.2, VeraSafe may, in its sole discretion, refer matters to appropriate government agencies if:*

a. the Participant refuses to comply with the Procedure in regard to a Complaint that has been filed with VeraSafe; or
b. VeraSafe determines that the Participant has failed to comply with a Settlement Agreement or Reparation Order issued under the Procedure within a reasonable time.

11.2*. Before referring any matter to the appropriate government agency, VeraSafe must first notify Participant of the intended referral and give Participant a reasonable opportunity of at least 10 business days to cure any breach or failure to perform under the Procedure.*
11.3*. Reports of referrals to government agencies shall be included in VeraSafe's Annual Procedure Report (defined below).*
11.4. *Where appropriate and possible, VeraSafe shall cooperate on complaint processing with other Accountability Agents, as needed, in accordance with the Applicable System Requirements.*

15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible and to potential requests from Privacy Enforcement Authorities (PEAS) s and relevant government entities of Members.

VeraSafe is committed to cooperating with enforcement entities in APEC economies, Privacy Enforcement Authorities (PEAs), and relevant government entities of Global CBPR Forum Members, as applicable, in a manner that aligns with applicable laws, regulatory obligations, and the principles of the CBPR (Cross-Border Privacy Rules) and PRP (Privacy Recognition for Processors) frameworks.

VeraSafe will respond to enforcement requests that:

- reasonably relate to the requesting APEC economy or Global CBPR Forum Member, as applicable, and its jurisdiction over CBPR- and/or PRP-related activities;
- concern a Participant's compliance with the CBPR or PRP programs in which the Participant is certified; and
- are legally permissible and do not conflict with VeraSafe's obligations under confidentiality agreements, data protection laws, or contractual commitments.

Where possible, VeraSafe will work in good faith to support enforcement entities while ensuring that responses remain proportionate, accurate, and compliant with applicable policies.

Step 1: Verification of Request

Upon receiving a request from an APEC enforcement entity, PEA or a relevant government entity of a Global CBPR Forum Member, as applicable, VeraSafe will:

- Confirm the identity and authority of the requesting entity.
- Determine the relevance of the request in relation to CBPR/PRP-related activities.
- Assess any legal or contractual obligations that may impact VeraSafe's ability to respond fully.

Step 2: Internal Review and Response Preparation

- VeraSafe will conduct an internal assessment to determine the scope of information it can provide while adhering to program policies and legal requirements.
- If the request involves a Participant's compliance status, VeraSafe will review certification records, prior compliance assessments, and relevant program documentation to formulate a response.
- If necessary, VeraSafe may notify the Participant about the request (subject to legal constraints) and provide them with an opportunity to respond or clarify their position.

Step 3: Response to the Enforcement Entity

- VeraSafe will provide a timely, accurate, and legally compliant response to the requesting authority.
- The response may include:
    - Confirmation of a Participant's certification status under the CBPR/PRP framework.
    - Details of any prior compliance assessments relevant to the request.
    - Information regarding VeraSafe's enforcement actions, if the request concerns a Participant that has been subject to penalties or certification suspension.
- If VeraSafe is unable to fulfill the request in full, it will communicate the reasons for such limitations and explore alternative ways to provide assistance.

Step 4: Ongoing Cooperation & Follow-Ups

- If further clarification or additional documentation is required, VeraSafe will continue to engage with the requesting authority as necessary.
- VeraSafe will track and document all enforcement requests received, and actions taken to ensure transparency and compliance with applicable policies.

Limitations on Enforcement Cooperation

VeraSafe will make reasonable efforts to cooperate with enforcement entities; however, it may be unable to provide information or assistance in cases where:

- The request exceeds the scope of VeraSafe's role as an Accountability Agent.
- Disclosing the requested information would violate data protection laws or confidentiality agreements.
- The request is unclear, lacks proper authorization, or originates from an entity outside an APEC economy or from an entity that is not member of the Global CBPR Forum, as applicable, and lacks an established legal basis for cooperation.

+1-617-398-7067
info@verasafe.com
www.verasafe.com

Appendix A

VeraSafe Conflicts of Interest Policy and Procedures for the APEC and Global CBPR and PRP Systems

+1-617-398-7067
info@verasafe.com
www.verasafe.com

Appendix B

VeraSafe CBPR and PRP Systems Dispute Resolution Procedure

+1-617-398-7067
info@verasafe.com
www.verasafe.com

Appendix C

VeraSafe Global CBPR Forum Certification Program Addendum

+1-617-398-7067
info@verasafe.com
www.verasafe.com