VeraSafe Privacy Program 2018 Annual Report

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

Contents

Executive Summary

This report covers the period from August 1, 2017 to July 31, 2018, which marked the second year of the operation of the VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Program as part of the VeraSafe™ Privacy Program™. VeraSafe is a trusted provider of data protection services to businesses and consumers in the United States and throughout the world. The VeraSafe Privacy Program (the "Privacy Program") is a comprehensive set of privacy assessment and compliance solutions that incorporates not only the requirements of the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework (collectively, the "Privacy Shield Frameworks" or "Privacy Shield"), but also prepares participating organizations for related privacy laws and frameworks. VeraSafe's assessment criteria align with the requirements of the General Data Protection Regulation of the European Union (GDPR).

By building a Privacy Shield Independent Resource Mechanism into the VeraSafe Privacy Program, VeraSafe has created the most complete set of privacy assessment and compliance solutions for the Privacy Shield Frameworks. From preliminary scoping and discovery, IT security reviews, data governance reviews, and third-party vendor negotiations to compliance remediation and guided Privacy Shield self-certification, participating organizations demonstrate a strong commitment to data protection and have invested considerable resources in satisfying VeraSafe's assessment criteria.

In the reporting period, VeraSafe clients ranging from tech startups to large multinational corporations received privacy compliance, dispute resolution, and privacy training services that fulfilled and surpassed the already high bar set by the Privacy Shield Frameworks.

About Privacy Shield

The General Data Protection Regulation of the European Union prohibits the transfer of personal data to countries outside the European Economic Area whose laws do not offer a level of data protection essentially equivalent to those of the EU. In a series of "adequacy" decisions, the European Commission identified so-called "third countries" whose national laws provide an adequate level of data protection for individuals and to which personal data of European origin could therefore be transferred without additional protections. In the absence of such an adequacy decision, an alternative data transfer mechanism is required in order to transfer personal data from an EEA member state to a third country.

Between 1998 and 2000, the United States Department of Commerce worked with the EU and Switzerland to develop the Safe Harbor Principles, intended to ensure the protection of personal data transferred from Europe to the United States. The European Commission issued a Decision (the "Safe Harbor Decision") in 2000 declaring that organizations participating in the Safe Harbor did provide an adequate level of data protection.

The Safe Harbor arrangement, the immediate precursor to the Privacy Shield Frameworks, was the transatlantic data transfer mechanism of choice until October 6, 2015, when the European Union Court of Justice invalidated the European Commission's Safe Harbor Decision.

The EU-U.S. Privacy Shield Framework came into effect on August 1, 2016, imposing stronger obligations on U.S. businesses to protect the personal data received in reliance on the Framework, increased oversight and enforcement powers on the part of the United States Department of Commerce, the United States Federal Trade Commission, and the United States Department of Transportation, and increased cooperation with European Data Protection Authorities, while still providing the same core principles of data protection that underpinned the Safe Harbor.

Like the Safe Harbor Frameworks before them, the Privacy Shield Frameworks require self-certification with the Department of Commerce. Participating businesses must certify that they adhere to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability, among other supplementary principles and binding arbitration requirements. Participants are required to maintain their self-certification on the official Privacy Shield List maintained by the Department of Commerce, to verify their self-certification annually via internal or third-party compliance assessment, and to provide independent dispute resolution via an "Independent Recourse Mechanism" (IRM). Qualified IRMs are required to provide unbiased dispute resolution services to individuals whose personal data is imported by Privacy Shield-certified entities in reliance on the Privacy Shield.

Statistical Overview for the 2017-2018 Reporting Period

Membership Statistics			
	VeraSafe Dispute Resolution Program (IRM)	VeraSafe Privacy Program (Verification)	Both Programs
Number of Member Organizations	78	23	23

Eligible Complaints			
Number of Eligible Complaints Received	Types of Complaints Received	Processing Time	Outcome
0	N/A	N/A	N/A

VeraSafe's Privacy Shield Independent Recourse Mechanism Services

VeraSafe, as a provider of Privacy Shield Independent Recourse Mechanism dispute resolution services, is responsible for providing unbiased mediation services to individuals with privacy grievances.

VeraSafe also provided dispute resolution services under the now-defunct Safe Harbor Program, and continues to serve former Safe Harbor clients for the purposes of any legacy complaints that might arise.

Offered as part of its Privacy Program, VeraSafe has created a Privacy Shield Dispute Resolution Procedure (the text of which is attached to this report as Exhibit A) that incorporates the Privacy Shield IRM requirements into a broader, balanced arbitration process designed to fully address privacy complaints from data subjects in Europe and throughout the world.

In the spirit of transparency, the full text of the Dispute Resolution Procedure is available on VeraSafe's public website. Data subjects who wish to submit a dispute concerning a VeraSafe Privacy Program Participant can easily do so at https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/.

VeraSafe Dispute Resolution Services are always provided free of charge to data subject complainants.

In its second year as an official Privacy Shield IRM provider, VeraSafe received no complaints from data subjects alleging a violation of data protection rights within the context of the Privacy Shield Frameworks.

The lack of Privacy Shield complaints meets VeraSafe's expected projections for Privacy Shield's second year of operation. As VeraSafe's Privacy Program exceeds the data protection requirements of the Privacy Shield Frameworks, Participants in the Privacy Program achieve not

only Privacy Shield compliance, but also graduate from our assessment with a mature data protection program that aligns with the high standards of European data protection law and genuinely limits the opportunity for compliance issues to arise.

Participation Requirements

Participants agree to be bound by the terms of the VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure, located at https://www.verasafe.com/privacy-services/dispute-resolution/privacy-shield-dispute-procedure.

Participants agree that VeraSafe, to the extent permitted by the Procedure, in its sole discretion as provider of independent Privacy Shield dispute resolution for the Participant, may impose fines against a Participant for its failure to comply with the Privacy Shield Framework(s), the Applicable Program Criteria, or the Procedure. Participants acknowledge that this is an essential aspect of the Recourse, Enforcement and Liability Principle of the Privacy Shield Frameworks and that it is the Participant's responsibility to pay fines and fees related to Privacy Shield disputes.

Each Participant further represents, warrants, and covenants to VeraSafe that:

- It has completed a third-party verification or a self-verification of its compliance with the Privacy Shield Frameworks that satisfies the requirements of the supplemental principle on Verification of the Privacy Shield Frameworks or the FAQ on Verification of the Safe Harbor Frameworks, as applicable, and will maintain a data protection program that complies with the Privacy Shield Frameworks;
- It will review, be familiar with, and be bound by the terms and conditions of the Procedure found at: https://www.verasafe.com/privacy-services/dispute-resolution/privacy-shield-dispute-procedure/;
- It is not prohibited by law from participating in the Program

How to File a Complaint

A Complainant must provide certain information to VeraSafe in order to successfully file a Complaint with the Procedure. Therefore, the Complaint must:

- allege a Participant's failure to comply with the Framework(s);
- name a Participant that is in good standing in the Program(s) and that has listed VeraSafe as its independent dispute resolution mechanism on its EU-U.S. Privacy Shield, Swiss-U.S. Privacy Shield, U.S.-EU Safe Harbor, or U.S.-Swiss Safe Harbor self-certification(s) with the U.S. Department of Commerce, as a defendant in the Complaint;
- include the desired outcome(s) that are being sought;
- include the fullest possible account of facts and events giving rise to the Complaint;
- if any damages or harm is alleged, include specific details of the harm and/or damages;

- include valid contact information for the Complainant;
- include consent to share the Complaint with the Participant;
- include all available documentation to support the Complaint; and
- include a declaration, under penalty of perjury under the laws of the United States of America, that all information submitted to VeraSafe in the Procedure is true and correct.

The Complainant is not required to pay any remuneration to VeraSafe in order to file a complaint with the Procedure.

Complaints must be initiated by submitting VeraSafe's online complaint form located at: https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/ or by submitting the required information to VeraSafe via fax.

VeraSafe shall provide correspondence to the Parties electronically, either by email or fax. The Parties shall submit all information, correspondence, and other material required by, or intended for use in, the Procedure ("Procedure Submissions") to VeraSafe electronically. Procedure Submissions shall be considered delivered to the recipient immediately upon their electronic transmission by the sender.

Complaint Handling Procedures

Eligibility

For a Complainant to be eligible to file a Complaint with the Procedure, the Complainant must be:

- above twelve years of age at the moment the Complaint is filed with the Procedure; and
- the Data Subject of PII exported from the EEA or Switzerland by or to a Participant; or
- the parent or legal guardian of a Data Subject who is under eighteen years of age at the time that the Complaint is filed with VeraSafe and whose PII was exported from the EEA or Switzerland by or to a Participant.

For a Complaint to be eligible under the VeraSafe Privacy Shield Dispute Resolution Procedure, the Complaint must include the required information described in Section 3.1 of the VeraSafe Privacy Shield Dispute Resolution Procedure and must:

- not have been previously resolved or settled by court action, arbitration, or other form of dispute resolution;
- not seek relief or other outcomes beyond the Procedure's Permitted Outcomes; and
- be filed with the Procedure for the first time, except for Complaints alleging a Participant's failure to comply with a previous Settlement Agreement.

The Complainant must make a good faith effort to resolve his dispute directly with the Participant before filing the Complaint with VeraSafe. Complainants are further encouraged to

read the Participant's privacy notice(s) entirely before filing a Complaint with VeraSafe. If VeraSafe determines, in its sole discretion, no good faith effort to resolve the dispute has been made, VeraSafe shall ask the Complainant to try to resolve the Complaint directly with the Participant and shall advise the Complainant that he may re-file the Complaint with the Procedure, as outlined herein, if the attempt to resolve the Complaint with the Participant does not yield satisfactory results.

If VeraSafe, in its sole discretion, concludes that additional information is needed to sustain a Complaint, it shall promptly contact the Complainant and advise him of the need for further information. If VeraSafe does not receive the requested information within fifteen business days of its request, VeraSafe shall close the Complaint, record an outcome of "Ineligible," and notify the Complainant of the outcome.

If, based on the information available to VeraSafe, the Complaint or Complainant is found to be ineligible (an "Ineligibility Determination"), VeraSafe shall close the Complaint, record an outcome of "Ineligible," and notify the Complainant of the outcome.

The Complainant has the right to appeal VeraSafe's Ineligibility Determination within ten business days of receiving the Ineligibility Determination. If the Complainant can furnish Credible Evidence to VeraSafe that a material error was made in the Ineligibility Determination, VeraSafe shall duly re-examine the Complaint and make a final determination as to the eligibility of the Complaint and Complainant.

Permitted Outcomes

The VeraSafe Privacy Shield Dispute Resolution Procedure provides for the following outcomes for complaints lodged thereunder:

- *the effects of noncompliance with the Framework(s) to be reversed or corrected by the Participant;*
- *that future data processing by the Participant be in conformity with the Framework(s);*
- *that the Participant cease processing PII of the Complainant;*
- *the Participant to delete relevant PII that was processed contrary to the Framework(s);*
- *the temporary suspension and/or removal of Participant's license to display VeraSafe Seal(s);*
- *the Participant to compensate the Complainant for actual, direct losses incurred as a result of Participant's non-compliance with the Framework(s); or*
- *the Participant to comply with other injunctive orders.*

Privacy Shield, the GDPR, and Beyond

When VeraSafe set out to create the Privacy Program, it did so with the intent to provide a holistic solution to the privacy needs of U.S. businesses. Rather than constrain the Privacy Program by basing it on the tenets of the Privacy Shield Frameworks, VeraSafe chose to create a comprehensive, forward-looking privacy solution more heavily aligned with the higher standards of the GDPR than Privacy Shield itself.

The result was the VeraSafe Privacy Program Certification Criteria (the "Program Criteria"), the full text of which is available on VeraSafe.com (https://www.verasafe.com/privacy-services/certification-standard/) and included as Exhibit B to this Annual Report.

The higher bar set by VeraSafe's Privacy Program is particularly relevant in light of Opinion 01/2016, handed down by the Article 29 Data Protection Working Party (WP29) (an independent European advisory body on data protection and privacy) that highlights various ways in which the Privacy Shield Frameworks can be improved upon.[1]

While the WP29 praised the improvements that Privacy Shield made over the older Safe Harbor scheme, it also identified numerous areas where improvement was needed. VeraSafe took these recommendations into account when creating and updating the Program Criteria, which resulted in a set of compliance criteria that more fully reflect the intent of European data privacy law.

VeraSafe's Privacy Program goes beyond a strict interpretation of the Privacy Shield Frameworks and attempts to bridge the gap between Privacy Shield and the forthcoming GDPR in multiple ways.

A Marriage of Privacy and Security Standards

Cognizant of the need for sophisticated data security standards, VeraSafe incorporated existing technological and informational security standards into the Program Criteria to ensure that each Privacy Program assessment is conducted with exceptional rigor and attention to detail.

The Program Criteria is a highly actionable set of requirements that merges the Privacy Shield Framework's principles with the U.S. National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF).

A More Expansive View of the Right of Access

In the context of the Access Principle, the Privacy Shield Frameworks take a narrower view of a data subject's right to access his or her personal data. As the WP29 has pointed out in Opinion 01/2016, Supplemental Principle 8 of Privacy Shield states that "access needs to be provided only to the extent that an organization stores the personal information."[2] This focus on "storage" of personal data misleadingly limits the actual definition of "processing" under European privacy law, which includes many other activities and operations performed on personal data by an organization. Under both the European Data Protection Directive and the GDPR, data subjects have a right to access their personal data with regard to all types of processing, not only data storage.

---

[1] Article 29 Data Protection Working Party Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision.

[2] Privacy Shield Annex II, III.8.d.ii.

VeraSafe has taken this more expansive view of data processing into account in its Program Criteria, which align with the access principles of the GDPR.

Best in Class Privacy Training Requirements and Solutions

In order to verify the effectiveness of an organization's commitment to comply with the Privacy Shield Frameworks, organizations are required to make either a self-assessment or engage in an outside compliance review, such as that offered by VeraSafe.

While the Privacy Shield Frameworks only require organizations to verify that they have implemented appropriate employee privacy training when they have chosen a self-assessment, VeraSafe requires all organizations that participate in its Privacy Program to comply with the following training requirements:

- *Awareness and Training. [PR.AT]*
    - *Implement and maintain a data-security-training-program for all employees within the Scope of the Certification.*
    - *Implement and maintain an ongoing data-security-awareness-program for all employees within the Scope of the Certification.*

This training requirement is not otherwise inherently required of organizations that have opted to undergo an outside compliance review.

In an effort to provide employee training resources on the topics of privacy and data security to all companies who desire it, VeraSafe has developed PrivacyTrain, a web-based software application located at PrivacyTrain.com. PrivacyTrain is a unique, powerful tool that helps organizations provide and track training for their employees and serves as a platform for high-quality, engaging privacy and security training content developed in-house at VeraSafe.

Clarity on the Roles of Controllers and Processors

A major ambiguity the WP29 pointed out in the current iteration of the Privacy Shield Frameworks relates to the application of the Privacy Shield to U.S. organizations acting as data processors on behalf of EU data controllers:

> "The extent to which the Privacy Shield Principles are applicable to certified organisations receiving personal data from the EU for mere processing purposes (referred to as 'Agents' or 'processors') unfortunately remains unclear. While the provisions under Annex II, III.10.a. do mention data transfers to certified organisations for such purposes - i.e. mentioning the requirement to enter into a contract - they lack any indication as to how the Privacy Shield Principles shall apply to processors (Agents). This causes uncertainty both for the certified U.S. organisations receiving data for processing purposes and for EU companies carrying out data transfers to certified organisations acting as data processors, as well as for the individuals whose data are processed. **In consequence, it will be difficult to determine which duties actually apply to Shield organisations processing personal data received from the EU in their role as processors. Clarification is therefore certainly required.**"[3]

VeraSafe provides the necessary clarity in its Privacy Program Certification Criteria: the Program Criteria clearly designate each obligation as being applicable to either data controllers, data processors, or both, in line with the approach taken by the GDPR.

Data Destruction Requirements

While the Privacy Shield Frameworks omit the requirement, inherent in EU privacy law, that a data controller must ensure that personal data is deleted once the purpose for which it was collected or further processed becomes obsolete, VeraSafe places this obligation on all Participants who qualify as data controllers.

Impact of the GDPR

Since May 25, 2018, when the GDPR formally came into full force and effect, VeraSafe has observed steady interest in its Privacy Shield-related service offerings, suggesting that U.S. businesses continue to view the Privacy Shield as a valuable tool in the pursuit of their European business interests.

Conclusion

VeraSafe has set forth a data protection standard that incorporates the requirements of the Privacy Shield Frameworks, the views of the Article 29 Working Party, and the NIST CSF.

[3] WP29 Opinion 01/2016 at page 16 (emphasis added).

VeraSafe considers that upon successful completion of our Privacy Program assessment, organizations are particularly well equipped to protect personal data and to protect the fundamental rights and freedoms of their data subjects. VeraSafe is pleased by the fact that organizations participating in our programs have not been subject to any qualified Privacy Shield-related complaints in the reporting period.

Contact VeraSafe

Questions about this report can be directed to the following members of VeraSafe's data protection practice:

Matthew Joseph, CIPP/E, CIPP/US
matt@verasafe.com

James Cormier, CIPP/E
Senior Counsel
jim@verasafe.com

VeraSafe U.S.:

VeraSafe
P.O. Box 8203
Essex, VT 05451 USA

VeraSafe EU:

VeraSafe Czech Republic
Zahradníčkova 1220/20A
Prague 15000
Czech Republic

EXHIBIT A

VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure

Last Updated: May 30, 2017

1. Introduction.

1.1. The VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure (the "Procedure") is provided and administered by Advanced Partnerships LLC ("VeraSafe") for the resolution of complaints alleging that a Participant in the VeraSafe Privacy Program or VeraSafe Privacy Shield/Safe Harbor Dispute Resolution Program (the "Program(s)"), who is also subject to the EU-U.S. Privacy Shield Framework, Swiss-U.S. Privacy Shield Framework, U.S-EU Safe Harbor Framework, or U.S.-Swiss Safe Harbor Framework, has failed to comply with the Framework(s). The Procedure combines facilitation, mediation, and arbitration.

1.2. VeraSafe commits to comply with the requirements for independent recourse mechanisms as set forth in Principle 7 "Recourse, Enforcement and Liability" and Supplemental Principle 11 "Dispute Resolution and Enforcement" of the Privacy Shield Framework and the Enforcement Principle and FAQ 11 "Dispute Resolution and Enforcement" of the Safe Harbor Frameworks. In case of a conflict between the Procedure and one of the Frameworks, the relevant Framework(s) shall control, and the Procedure shall be modified to the minimum extent necessary in order to permit VeraSafe to comply with its obligations as an independent recourse mechanism under the Framework(s).

1.3. By participating in the Procedure, the Parties agree to the terms and conditions of the Procedure as set forth herein.

2. Definitions.

2.1. The following definitions apply to the Procedure:

a. "Appellate Hearing" means the process described under Section 9 of the Procedure.
b. "Complainant" means a person who has filed, or attempted to file, a Complaint with VeraSafe under the terms of the Procedure.
c. "Complaint" means an allegation of non-compliance with the EU-U.S. Privacy Shield Framework, Swiss-Privacy Shield Framework, U.S.-EU Safe Harbor Framework, or U.S.-Swiss Safe Harbor Framework registered with VeraSafe under the terms of the Procedure.
d. "Credible Evidence" means facts that, when viewed in light of surrounding circumstances, are highly and substantially likely to be true.
e. "EEA" means the European Economic Area.
f. "Framework(s)" means the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, the U.S.-EU Safe Harbor Framework, and the U.S.-Swiss Safe Harbor Frameworks.
g. "Participant" means a member of the VeraSafe Privacy Program or VeraSafe Privacy Shield/Safe Harbor Dispute Resolution Program.
h. "Party/Parties" means the Complainant or the Participant, or both as applicable.
i. "Procedure Submissions" means all documents, writings, briefs, evidence and other material, submitted to the Procedure by the Parties or by VeraSafe.
j. "Settlement Agreement" means an agreement reached by the Parties that resolves the Complaint. The terms of such agreement must be recorded in writing to be effective.

2.2. Capitalized terms not defined herein shall be understood to have the same meaning as ascribed to such terms in the VeraSafe Privacy Program Certification Criteria.

3. Complaint Filing Procedure.

3.1. Information Required. A Complainant must provide certain information to VeraSafe in order to successfully file a Complaint with the Procedure. Therefore the Complaint must:

a. allege a Participant's failure to comply with the Framework(s);
b. name a Participant that is in good standing in the Program(s) and that has listed VeraSafe as its independent dispute resolution mechanism on its EU-U.S. Privacy Shield, Swiss-U.S. Privacy Shield, U.S.-EU Safe Harbor, or U.S.-Swiss Safe Harbor self-certification(s) with the U.S. Department of Commerce, as a defendant in the Complaint;
c. include the desired outcome(s) that are being sought;
d. include the fullest possible account of facts and events giving rise to the Complaint;
e. if any damages or harm is alleged, include specific details of the harm and/or damages;
f. include valid contact information for the Complainant;
g. include consent to share the Complaint with the Participant;
h. include all available documentation to support the Complaint; and
i. include a declaration, under penalty of perjury under the laws of the United States of America, that all information submitted to VeraSafe in the Procedure is true and correct.

3.2. The Complainant is not required to pay any remuneration to VeraSafe in order to file a complaint with the Procedure.

3.3. Medium for all Procedure Submissions.

a. Complaints must be initiated by submitting VeraSafe's online complaint form located at: https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/ or by submitting the required information to VeraSafe via fax.
b. VeraSafe shall provide correspondence to the Parties electronically, either by email or fax.
c. The Parties shall submit all information, correspondence, and other material required by, or intended for use in, the Procedure ("Procedure Submissions") to VeraSafe electronically.
d. Procedure Submissions shall be considered delivered to the recipient immediately upon their electronic transmission by the sender.

4. Permitted Outcomes.

4.1. The Parties agree that the possible outcomes that a Complainant may seek via the Procedure, and the maximum relief that VeraSafe shall assign in a Data Privacy Hearing (as such term is defined in Section 8) or Appellate Hearing during the Procedure are limited to the outcomes described below (the "Permitted Outcomes"). Permitted Outcomes are only those that may require:

a. the effects of noncompliance with the Framework(s) to be reversed or corrected by the Participant;
b. that future data processing by the Participant be in conformity with the Framework(s);
c. that the Participant cease processing PII of the Complainant;
d. the Participant to delete relevant PII that was processed contrary to the Framework(s);
e. the temporary suspension and/or removal of Participant's license to display VeraSafe Seal(s);
f. the Participant to compensate the Complainant for actual, direct losses incurred as a result of Participant's non-compliance with the Framework(s); or
g. the Participant to comply with other injunctive orders.

5. Eligibility.

5.1. Eligible Complainant. For a Complainant to be eligible to file a Complaint with the Procedure, the Complainant must be:

a. above twelve years of age at the moment the Complaint is filed with the Procedure; and
b. the Data Subject of PII exported from the EEA or Switzerland by or to a Participant; or
c. the parent or legal guardian of a Data Subject who is under eighteen years of age at the time that the Complaint is filed with VeraSafe and whose PII was exported from the EEA or Switzerland by or to a Participant.

5.2. For a Complaint to be eligible under the Procedure, the Complaint must include the required information described in Section 3.1 and must:

a. not have been previously resolved or settled by court action, arbitration, or other form of dispute resolution;
b. not seek relief or other outcomes beyond the Procedure's Permitted Outcomes; and
c. be filed with the Procedure for the first time, except for Complaints alleging a Participant's failure to comply with a previous Settlement Agreement.

5.3. Prior Good Faith Attempt to Resolve Complaint. The Complainant must make a good faith effort to resolve his dispute directly with the Participant before filing the Complaint with VeraSafe. Complainants are further encouraged to read the Participant's privacy notice(s) entirely before filing a Complaint with VeraSafe. If VeraSafe determines, in its sole discretion, no good faith effort to resolve the dispute has been made, VeraSafe shall ask the Complainant to try to resolve the Complaint directly with the Participant and shall advise the Complainant that he may re-file the Complaint with the Procedure, as outlined herein, if the attempt to resolve the Complaint with the Participant does not yield satisfactory results.

5.4. If VeraSafe, in its sole discretion, concludes that additional information is needed to sustain a Complaint, it shall promptly contact the Complainant and advise him of the need for further information. If VeraSafe does not receive the requested information within fifteen business days of its request, VeraSafe shall close the Complaint, record an outcome of "Ineligible," and notify the Complainant of the outcome.

5.5. Ineligibility Determination. If, based on the information available to VeraSafe, the Complaint or Complainant is found to be ineligible (an "Ineligibility Determination"), VeraSafe shall close the Complaint, record an outcome of "Ineligible," and notify the Complainant of the outcome.

a. **Complainant's Right to Appeal the Ineligibility Determination.** The Complainant has the right to appeal VeraSafe's Ineligibility Determination within ten business days of receiving the Ineligibility Determination. If the Complainant can furnish Credible Evidence to VeraSafe that a material error was made in the Ineligibility Determination, VeraSafe shall duly re-examine the Complaint and make a final determination as to the eligibility of the Complaint and Complainant.

6. Complainant's Noncompliance With The Procedure.

6.1. If the Complainant breaches any term(s) of the Procedure in a material way, VeraSafe has the right to close the Complaint, record an outcome of "Closed by Default," and duly notify the Parties.

7. Consultative Mediation.

7.1. Participant's Response To Complaint. Complaints that VeraSafe determines to be eligible shall be forwarded by VeraSafe to the Participant. The Participant must file its response to the Complaint ("Response to Complaint") with VeraSafe within twenty business days of its receipt of the Complaint. The Participant's Response to Complaint must either:

a. defend the Participant's actions as permitted under the Framework(s);

b. dispute the validity of information presented in the Complaint and contain all available documentation to support the dispute; or
c. admit fault and agree to remedy the alleged violation(s).

7.2. Participant's Failure to Respond. If the Participant fails to file a timely Response to Complaint, the failure to comply with the Procedure will be duly noted in the next Annual Procedure Report (as such term is defined in Section 14 of the Procedure) and VeraSafe shall refer the matter to the appropriate government agency in accordance with Section 13 of the Procedure.

7.3. Upon VeraSafe's receipt thereof, the Participant's Response to Complaint will be forwarded to the Complainant.

a. **Mediation Teleconference.** If the Complainant is not satisfied by the Participant's Response to Complaint, the Complainant may file with VeraSafe, a request for a mediation session to be conducted via telephone (hereinafter, a "Mediation Teleconference") within ten business days of receiving the Participant's Response to Complaint. The Mediation Teleconference is an informal process for the Parties to re-examine the details of the Complaint and work towards a mutually agreeable resolution.
b. If the Complainant is satisfied by the Participant's Response to Complaint, the Complainant shall notify VeraSafe in writing that the Complaint is resolved.
c. If VeraSafe receives notification from the Complainant that the Complainant is satisfied with the Participant's Response to Complaint, or otherwise receives no request for a Mediation Teleconference from the Complainant within the timeframe specified in Section 6.3(a), VeraSafe shall close the complaint with an outcome of "Closed by Default" and duly notify the Parties.

7.4. Mediation Teleconference Procedure. VeraSafe will provide and appoint a mediator to lead the Mediation Teleconference. VeraSafe will make a reasonable effort to schedule the teleconference with due regard for the schedules of the Parties and will notify the Parties of the scheduled time and date not less than fifteen days prior to the date of the Mediation Teleconference.

a. **Possible Outcomes of the Mediation Teleconference.** VeraSafe will provide and appoint a mediator to lead the Mediation Teleconference. VeraSafe will schedule the teleconference with due regard for the schedules of the Parties and will notify the Parties of the scheduled time and date no less than 15 days prior to the scheduled Mediation Teleconference. The Mediation Teleconference is an informal process to re-examine the Complaint and guide the Parties towards a mutually agreeable solution or settlement.
    I. **Complainant's Failure to Comply.** If the Complainant fails to appear at the scheduled time of the Mediation Teleconference, it will be assumed that the Participant's Response to Complaint has satisfied the Complainant and the Complaint will be closed with an outcome of "Closed by Default" and the Parties duly notified.
    II. **Participant's Failure to Comply.** If the Participant fails to appear at the scheduled time of the Mediation Teleconference, such failure to comply with the Procedure will be duly noted in the next Annual Procedure Report and VeraSafe shall refer the matter to the appropriate regulatory agency in accordance with Section 13.
    III. **Mutual Settlement Agreement.** If the Parties reach an agreement during the Mediation Teleconference, VeraSafe will record the Settlement Agreement parameters and notify both Parties in writing of the terms of the Settlement Agreement as decided by the Parties, within five business days of the Mediation Teleconference or as soon as reasonably practicable thereafter.
    IV. **No Settlement Reached.** If no Settlement Agreement is reached during the Mediation Teleconference, the Complainant may file with VeraSafe, a request for a Data Privacy Hearing within ten business days of the Mediation Teleconference.
    V. If no Settlement Agreement is reached during the Mediation Teleconference, and the Complainant does not request a Data Privacy Hearing within ten business days of the Mediation Teleconference, the Complaint will be closed with an outcome of "Closed by Default" and the Parties duly notified.

8. Data Privacy Hearing.

8.1.Overview. Upon the request of the Complainant made to VeraSafe in accordance with the requirements of the Procedure, an officer appointed by VeraSafe will review the Complaint and all Procedure Submissions in a fair and impartial way and determine if clear, convincing, and satisfactory evidence is present to support the alleged violation of the Framework(s) made in the Complaint (a "Data Privacy Hearing").

8.2. Exchange of Brief and Rebuttal. The Complainant's request for a Data Privacy Hearing should include its detailed brief of the Complaint. Upon receipt, VeraSafe will forward the brief to the Participant. The Participant shall provide a rebuttal to VeraSafe within ten business days of receiving the Complainant's brief.

8.3. Data Privacy Hearing Officer.

a. The Data Privacy Hearing officer shall hold a current Certified Information Privacy Professional or Certified Information Privacy Manager credential from the International Association of Privacy Professionals, hold a Juris Doctor degree from an American Bar Association accredited law school, or be currently licensed to practice law in a jurisdiction of the United States or an EEA member state.
b. The Data Privacy Hearing officer shall be impartial and neutral in the application of the Procedure.

8.4. Data Privacy Hearing Administration and Procedure.

a. **Data Privacy Hearing Officer's Request for Information.**
    I. The Data Privacy Hearing officer may request additional information or seek clarification from either Party, or both Parties, regarding the Procedure Submissions.
    II. **Late Filings and Extensions.** If a Party submits required information after the specified time limits, the untimely information shall not be submitted to the Data Privacy Hearing officer unless VeraSafe grants an extension for good cause. In lieu of such untimely Procedure Submissions, the Data Privacy Hearing officer will proceed to use all other available Procedure Submissions in making its Hearing Decision.
b. **VeraSafe's Investigative Analysis.** During the Data Privacy Hearing, the VeraSafe Program Administrator will independently and impartially investigate the Procedure Submissions and furnish to the Data Privacy Hearing officer its analysis of the validity of each essential fact presented in the Procedure Submissions. Such VeraSafe investigative analysis shall then be included in the Data Privacy Hearing as a Procedure Submission.
c. **Hearing Decision and Burden of Proof.** The Hearing Officer shall examine the Procedure Submissions to decide if the available evidence does clearly, convincingly, and satisfactorily substantiate the allegation made in the Complaint and, if so, whether or not the alleged action or inaction of the Participant does violate the Framework(s) (the "Hearing Decision").
    I. **Substantiated Complaints.** If in due examination of the Procedure Submissions, and in due consideration of the totality of the circumstances, the Data Privacy Hearing officer determines that the available evidence does clearly, convincingly, and satisfactorily substantiate the allegation made in the Complaint, and that the action or inaction of the Participant does violate the Framework(s), the Data Privacy Hearing officer shall require the Participant to comply with one or more Permitted Outcomes, as appropriate under the circumstances (a "Reparation Order"). The Parties will be duly notified of the Reparation Order.
    II. **No Action Taken.** If, in due examination of the Procedure Submissions, and in due consideration of the totality of the circumstances, the Data Privacy Hearing officer determines that the available evidence does not clearly, convincingly, and satisfactorily substantiate the allegation made in the Complaint, or that the alleged action or inaction of the Participant does not violate the applicable Framework(s), the Complaint shall be closed with an outcome of "Closed – No Action Taken" and the Parties duly notified.

9. Right To Appeal.

9.1. Eligibility and Acceptance of Appeals.

a. Within ten business days of receiving notification that the Complaint has been closed with an outcome of "Closed – No Action Taken" the Complainant may submit an appeal to VeraSafe, if the Complainant believes that VeraSafe failed to adhere to the Procedure and such failure significantly affected the Hearing Decision.
b. To be considered, the appeal must include a detailed briefing of the alleged procedural error(s). VeraSafe will accept appeals when the Complainant's briefing presents Credible Evidence of a procedural error(s).

9.2. Brief and Rebuttal. Upon receipt of the appeal brief, VeraSafe will forward the appeal brief to the Participant. The Participant must provide a rebuttal to VeraSafe within ten business days of receiving the Complainant's appeal brief.

9.3. Appellate Hearing Officer. VeraSafe will appoint an officer to administer the Appellate Hearing using the eligibility criteria described in Section 8.3(a). The Appellate Hearing officer will not be the same individual as the Data Privacy Hearing officer that administered Section 8 of the Procedure.

9.4. Appellate Hearing Administration and Procedure.

a. **Appellate Hearing Decision.**
b. **Examination of Evidence.** In its examination of the Procedure Submissions, the Appellate Hearing officer will use the Hearing procedure as described in Section 8.4(c).
    I. **Substantiated Complaints.** If, in due examination of the Procedure Submissions, and in due consideration of the totality of the circumstances, the Appellate Hearing officer determines that the available evidence does clearly, convincingly and satisfactorily substantiate the allegation made in the Complaint, and that the action or inaction of the Participant does violate the Framework(s), the Appellate Hearing officer will issue a Reparation Order requiring the Participant to comply with one or more Permitted Outcomes, as appropriate under the circumstances. The Parties will be duly notified of the Reparation Order.
    II. **No Action Taken.** If, in due examination of the Procedure Submissions, and in due consideration of the totality of the circumstances, the Appellate Hearing officer determines that the available evidence does not clearly, convincingly and satisfactorily substantiate the allegation made in the Complaint, or that the alleged action or inaction of the Participant does not violate the applicable Framework(s), the Complaint will be closed with an outcome of "Closed – No Action Taken" and the Parties duly notified.

10. Complainant's Right To Withdraw.

10.1. A Complainant has the right to withdraw its Complaint at any time during the Procedure by submitting to VeraSafe a request to withdraw the Complaint.

a. The Complaint will then be closed with an outcome of "Closed – Withdrawn" and the Parties duly notified.

11. Language.

11.1. VeraSafe shall conduct the Procedure in English but insofar as the Complainant is only able to read or write in a language other than English, VeraSafe shall make commercially reasonable efforts to provide translation services to the Complainant as necessary during the Procedure.

12. Participant's Performance Under A Settlement Agreement Or Reparation Order.

12.1. The VeraSafe Program Administrator shall monitor the Participant's compliance with Settlement Agreements and Reparation Orders issued under the Procedure.

a. (a) When the VeraSafe Program Administrator is satisfied with the Participant's performance of an applicable Settlement Agreement or Reparation Order issued under the Procedure, the Complaint will then be closed with an outcome of "Closed by Settlement," or "Closed by Performance of Reparation Order" and the Parties duly notified.

12.2. Participant's Non Compliance. If Participant fails to comply with a Settlement or Reparation Order issued under the Procedure, the failure to comply with the Procedure shall be duly noted in the next Annual Procedure Report and VeraSafe shall refer the matter to the relevant government agency pursuant to Section 13.

13. Referral To Government Agencies.

13.1. VeraSafe in its discretion, may refer matters to U.S. government regulatory agencies of competent jurisdiction, if:

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

13.2. Before referring any matter to a regulatory agency of competent jurisdiction, VeraSafe shall first notify the Participant of the intended referral and give the Participant a reasonable opportunity of at least ten business days to cure any breach of the Framework(s) or any failure to perform its obligations under the Procedure.

13.3. Reports of referrals to government agencies shall be included in VeraSafe's Annual Procedure Report.

13.4. Complaints that VeraSafe refers to a regulatory agency under this Section shall be closed with an outcome of "Closed by Referral to Regulatory Agency," and the Parties duly notified.

14. Public Reporting.

14.1. VeraSafe shall publish an annual report on the operation of the Procedure (each, an "Annual Procedure Report"). The Annual Procedure Reports shall:

a. include the types of Complaint outcomes arising under the Procedure;
b. include a statistical summary of the nature of Complaints filed with the Procedure during the reporting period;
c. include the number of Complaints filed with the Procedure during the reporting period;
    I. include a statistical summary of the number and nature of Settlement Agreements and Reparation Orders issued under the Procedure during the reporting period;
    II. include a statistical summary of the number and nature of Complaints deemed ineligible during the reporting period pursuant to Section 5, including the specific reason(s) for each Ineligibility Determination;
    III. for each Complaint which VeraSafe refers to a regulatory agency pursuant to Section 13, include a summary (including the Participant's name) of the nature and outcome of the Complaint;
d. include the minimum, maximum, and average time for Complaints to be closed under the Procedure during the reporting period; and
e. be published on VeraSafe's website, https://www.VeraSafe.com.

14.2. The Annual Procedure Report's statistical summaries shall be comprised solely of aggregate, anonymous data.

15. Confidentiality.

15.1. Other than the Hearing Decisions and except as noted in Sections 13 and 14, all Procedure Submissions, deliberations, meetings, proceedings, and writings of the Procedure shall be treated as confidential by VeraSafe.

15.2. Each Party must treat any information provided to them by VeraSafe as confidential, and must not make such information available to anyone other than those persons directly involved in the handling of the Complaint, except as allowed or required by applicable law or by the Framework(s).

16. LIMITATION OF LIABILITY.

16.1. EXCEPT IN THE CASE OF DELIBERATE WRONGDOING, AND EXCEPT TO THE EXTENT THAT SUCH A LIMITATION OF LIABILITY IS PROHIBITED BY APPLICABLE LAW OR BY THE FRAMEWORK(S), AND WITH THE KNOWLEDGE THAT VERASAFE IS PROVIDING THE PROCEDURE FOR THE BENEFIT OF THE PARTIES INVOLVED, THE PARTIES ACKNOWLEDGE AND AGREE THAT THE FOLLOWING ARE NOT LIABLE FOR ANY ACT OR OMISSION IN CONNECTION WITH THE PROCEDURE: VERASAFE NOR ANY VERASAFE EMPLOYEE, BOARD MEMBER, COMPANY OFFICER, OR INDEPENDENT CONTRACTOR UTILIZED BY VERASAFE IN THE PROCEDURE.

16.2. VeraSafe can offer no guarantee that the outcome of the Procedure will be an outcome with which either Party, or the Parties, is satisfied.

17. Interpretation.

17.1. This Procedure shall be interpreted under the laws of the United States of America.

18. Waiver Of Subpoena.

18.1. Each Party agrees that it will not subpoena any of the following in any legal proceeding arising out of the Procedure or any Complaint: VeraSafe nor any VeraSafe employee, board member, company officer, or independent contractor utilized by VeraSafe in the Procedure.

19. Hold Harmless.

19.1. The Participant agrees to hold VeraSafe, its officers, agents and employees harmless from any liability, loss, or damage the Participant may suffer as a result of Complaints, claims, demands, costs, Settlement Agreements, Reparation Orders, or judgments against them arising out of the Procedure.

19.2. The Complainant agrees to hold VeraSafe, its officers, agents and employees harmless from any liability, loss, or damage the Complainant may suffer arising out of the Procedure or the acts or omissions of the Participant that gave rise to the Complaint.

20. Relationship Of The Parties.

20.1. Nothing contained in the Procedure shall be construed to create the relationship of principal and agent, partnership, or joint venture, or any other commercial relationship between VeraSafe and either Party.

20.2. The Parties have no authority to act as agent for, or on behalf of, VeraSafe, or to represent VeraSafe, or bind VeraSafe in any manner.

21. Contact Information.

21.1. VeraSafe may be contacted using the contact information found at https://www.VeraSafe.com/contactus.

21.2. The International Trade Administration of the U.S. Department of Commerce may be contacted via the website https://www.privacyshield.gov and http://export.gov/safeharbor/.

21.3. VeraSafe is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission. The Commission may be contacted using the information found on the website https://www.ftc.gov/contact.

EXHIBIT B

VeraSafe Privacy Program Certification Criteria
Rev. 13

Last Updated: May 30, 2017

Introduction

1. The VeraSafe Privacy Program Certification Criteria establish a baseline of data protection controls and fair information practices that must be implemented by Participants of the VeraSafe Privacy Program. The Program Criteria are based on prominent privacy legislation and various related frameworks, such as the General Data Protection Regulation (GDPR), the EU-U.S. Privacy Shield Framework, the National Institute of Standards and Technology Cybersecurity Framework, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the California Online Privacy Protection Act, the APEC Cross Border Privacy Rules, and the FTC Fair Information Practice Principles.
2. For a Participant to become certified in the Program, it must be a private body (i.e., not a government agency), and must satisfy these Program Criteria, pass the Verification Process as described in these Program Criteria, and attest to its compliance with these Program Criteria. Statements that a Participant publishes regarding its data governance and data security practices are enforceable by law in the United States and may be enforceable by relevant data protection or consumer protection authorities in other jurisdictions.
3. VeraSafe will issue its Privacy Seal to a Participant of the Program that successfully passes the Verification Process, attests to its compliance with these Program Criteria and is in good standing in the Program. Any Data Subject who believes that a Participant has failed to abide by these Program Criteria, can send a complaint to VeraSafe per the terms of the applicable VeraSafe dispute resolution procedure.

Definitions

The following definitions apply to these Program Criteria:

1. "Basis for Processing" means those grounds, as applicable, that are described in Section 3.1 and Section 3.2.
2. "Commercial Email Message" means an email message that advertises or promotes a commercial product or service, including content on a website operated for a commercial purpose.
3. "Consent" means a freely given, specific, and informed indication of authorization by the Data Subject (which, in the context of this definition, shall mean the parent or legal guardian of a Data Subject where the Data Subject is under the age of thirteen), either by a statement or by a clear affirmative action by the Data Subject, ensuring that the Data Subject is aware that they give their consent to the Processing of PII, including by ticking a box or by any other statement or conduct which clearly indicates, in the context, the Data Subject's agreement to the proposed Processing of their PII.
    a. Silence or inactivity of the Data Subject does not constitute valid Consent.
    b. The Data Controller must document the Consent provided by the Data Subject in sufficient detail to confirm the validity of the Consent and the specific purposes of Processing for which the Consent was provided by the Data Subject.

    c. It must be as easy for the Data Subject to withdraw Consent as it was for the Data Subject to give Consent.
    d. If the Data Subject's Consent is obtained in the context of a written document which also concerns other matters, the request for Consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear language that a reasonable person would comprehend.
4. "Data Breach" means the accidental, unlawful, or otherwise prohibited destruction, loss, alteration, unauthorized disclosure of, or access to, PII undergoing Processing.
5. "Data Controller" means a natural or legal person, public authority, agency, or any other body that, alone or jointly with others, determines the purposes and means of the Processing of PII.
6. "Data Processor" means a natural or legal person, public authority, agency, or any other body that Processes PII on behalf of a Data Controller.
7. "Data Subject" means a natural person that is described by PII.
8. "Information Society Service" means any data Processing service provided upon request, by electronic means, and without the need for the service provider and requestor to be simultaneously physically present in a single location.
9. "IT System" means any electronic data Processing equipment, system(s), or subsystem(s) within the Scope of the Certification.
10. "Participant" means the natural person, business, or other private legal entity that has entered into an agreement with VeraSafe to participate in the Program and certify its compliance with these Program Criteria.
11. "PII" means any data, information, or combination of data and information that can be used to identify or locate a specific individual natural person. This includes names, contact information, Social Security numbers and other national identification numbers, precise location data, and other individually identifiable data. PII does not include data or information that is manifestly made public at the will of the Data Subject.
12. "Privacy Notice" means the fair processing information provided by the Participant to Data Subjects, particularly pursuant to Section 2 of the Program Criteria. A compliant Privacy Notice may be provided in up to three non-contradictory layers, such as:
    a. a single comprehensive notice of the Participant's data Processing practices that, by and of itself, satisfies the requirements of Section 2 of the Program Criteria; and
    b. a summary notice highlighting the Participant's data Processing practices, and which provides a link to the comprehensive Privacy Notice; and
    c. disclosure of specific data Processing practices, posted at the point of PII collection.
13. "Privacy Seal" means the VeraSafe privacy seal(s) in digital form, as shown in the VeraSafe user control panel.
14. "Privacy Shield Framework" means the EU-U.S. Privacy Shield Framework, which is a binding framework for data protection promulgated by the U.S. Department of Commerce and the European Union ("EU") authorities, that regulates how participating U.S. companies Process PII.
15. "Privacy Shield List" means the publicly available list, maintained by the U.S. Department of Commerce, of organizations that have notified the U.S. Department of Commerce that they comply with the EU-U.S. Privacy Shield Framework.
16. "Privacy Shield Principles" means the list of requirements necessary for compliance with the Privacy Shield Framework as set forth at: https://www.privacyshield.gov/EU-US-Framework
17. "Procedure" means the VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure or the VeraSafe Dispute Resolution Procedure, as applicable." (see 1.1 at https://www.verasafe.com/privacy-services/dispute-resolution/privacy-shield-dispute-procedure/).
18. "Process" means any operation or set of operations which is performed on PII, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
19. "Program" means the VeraSafe Privacy Program.
20. "Program Criteria" means these VeraSafe Privacy Program Certification Criteria.

21. "Relationship Message" means an email message, the primary purpose of which:
    a. is to facilitate, complete or confirm a commercial transaction that the Data Subject has previously agreed to enter into with the Participant; or
    b. is to provide warranty or product recall, safety, or security information about a product or service purchased by the Data Subject; or
    c. pertains to subscription, membership, or other types of ongoing relationships; or
    d. pertains to an existing employment relationship; or
    e. pertains to the delivery of goods or services including product upgrades which the Data Subject is entitled to receive based upon a prior commercial relationship with the Participant.
22. "Secured Facility(s)" means the physical premises and the interior of a structure (or structures) to which the physical security controls are applied.
23. "Security Incident" means any attempted or actual Data Breach(es).
24. "Sensitive PII" means PII that describes or pertains to race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetics or data concerning health, sexual orientation, sex life, or criminal convictions as well as any data received from a Third Party where the Third Party treats and identifies it as Sensitive PII. Sensitive PII does not include data or information that is manifestly made public at the will of the Data Subject.
25. "Third Party" means any entity that is not the Participant or the Data Subject.
26. "Verification Process" means VeraSafe's observations, automated security scans, manual security evaluations and checks, evaluation of a Participant's questionnaire and survey responses, VeraSafe's independent verification of certain questionnaire and/or survey responses, and VeraSafe's analysis of documents provided by the Participant, which collectively are used to verify a Participant's compliance with the Program Criteria.
27. "Vital Interests" means matters of life and death.
28. "Workstation" means an electronic computing device and the electronic media stored in its immediate environment, for example, a laptop computer, desktop computer, smartphone, or any other device that performs similar functions, typically for one user at a time, and which Processes or which may be used to Process PII.

Data Protection Requirements

1. Scope Of The Certification.

1.1. The scope of each Participant's certification in the Program, to which the Program Criteria will be binding (hereinafter "Scope of the Certification"), must be clearly defined by the Participant.

1.2. The Scope of the Certification shall be foremost defined in terms of specific information system(s).

a. The Program Criteria are, therefore, applicable to the people, processes, hardware, software, and networks that comprise those information systems in the Scope of the Certification.

1.3. Data Controllership. For each information system within the Scope of the Certification, it must be defined whether the Participant is a Data Controller or a Data Processor.

a. If a Participant acts in two separate capacities (i.e., Data Controller and Data Processor) within the same information system, the circumstances of each role must be defined.

2. Notice.

2.1 Participants must implement, maintain, and publish a Privacy Notice(s) that complies with these Program Criteria.

a. The Privacy Notice(s) may be provided in a single document, or a series of compatible, layered Privacy Notices.
b. Multiple information systems in the Scope of the Certification may share a single (or a series of layered) Privacy Notice(s), insofar as the Program Criteria are satisfied for every information system contemplated by such Privacy Notice(s).

2.2 Required Privacy Notice Elements for Data Processors. Where the Participant is a Data Processor, that Participant's Privacy Notice(s) must:

a. be furnished to the Data Subject or be conspicuously displayed by the Participant; and
b. be presented in a legible format; and
c. be materially correct and up to date; and
d. state the date that the Privacy Notice came into effect (or was last materially revised, whichever is later); and
e. be written in clear language that a reasonable person would comprehend; and
f. be made available in the language(s) in which the Participant usually conducts its affairs; and
g. include a title containing the word "privacy" (such as "Privacy Policy," "Privacy Notice," et cetera); and
h. state the full legal name of the Participant; and
i. state the information systems to which the Privacy Notice applies; and
j. with regards to the information systems mentioned in point (i) of this Section, state the Participant's role as defined in Section 1.3 above; and
k. state any subsidiary entities of the Participant that are included within the Scope of the Certification and to which the Privacy Notice also applies; and
l. state the categories of PII that the Participant Processes; and
m. state the categories of ways in which the Participant receives or collects PII; and
n. state the specific, limited purpose(s) for which the Participant does or intends to Process PII; and
o. state the Basis for Processing the PII and, where the Participant Processes PII on the basis of Section 3.1(a)(5), list the specific legitimate interests that are pursued; and
p. provide the categories, or the identities, of Third Parties to which the Participant does or intends to disclose PII; and
q. disclose, if applicable, that the Participant intends to transfer PII onward to a third country; and
r. disclose all applicable Choice, Access, and Privacy of Children rights of the Data Subject as described in Sections 5, 6, and 10 respectively, and how a Data Subject (or the parent or legal guardian of a Data Subject under the age of thirteen) may exercise those rights; and
s. disclose the Participant's policy for deleting PII after such time as the purpose or Basis for Processing of such PII becomes obsolete; and
t. where the information system(s) disclosed pursuant to 2.2(i) include an Information Society Service and where the Participant collects PII pertaining to a Data Subject's Internet activities over time and across Third Party Information Society Services, (for example, through the use of HTTP cookies, web beacons, locally shared objects, device recognition technologies, or similar technologies, collectively "Cookies") disclose how, if at all, the Participant's Information Society Service responds to web browser tracking preference expressions, such as "Do Not Track"; and
    1. Notwithstanding the foregoing, Participant may alternatively include a clear and conspicuous hyperlink to an Internet website containing a description, including the effects, of any program or protocol the Participant follows that offers Data Subjects the option to prevent such data collection.
u. state that the Participant has implemented and will maintain reasonable security controls to protect the confidentiality, integrity, and availability of PII it Processes; and
v. state that, if the Participant makes PII available to a Third Party, such Third Party will be required to implement and maintain reasonable security controls to protect the confidentiality, integrity, and availability of such PII; and

w. disclose that PII Processed by the Participant may be transferred to Third Parties pursuant to lawful requests by public authorities, including national security and/or law enforcement requests, and that Section 2.2(v) may not apply to such transfers; and
x. state how to contact the Participant with any inquiries or complaints, including at least a current and valid mailing address, email address, toll-free telephone number or toll-free fax number; and
y. state the name or title, and business contact information, of a natural person appointed by the Participant, such as a competent data protection officer, to respond to data protection related inquiries and complaints lodged by Data Subjects; and
z. state the maximum number of days it will take the Participant to respond to data protection related inquiries or complaints received from Data Subjects; and
aa. disclose the Participant's procedure for notifying Data Subjects of a change in the respective Privacy Notice; and
bb. disclose any particular consumer protection agency that regulates the Participant's Processing of PII; and
cc. disclose that VeraSafe is designated to address privacy complaints lodged against the Participant and, subject to the terms and conditions of the applicable VeraSafe dispute resolution Procedure, will provide appropriate recourse free of charge to Data Subjects.

2.3 Supplemental Privacy Notice Elements for Data Controllers. Where the Participant is a Data Controller, that Participant's Privacy Notice must comply with the Privacy Notice requirements for Data Processors in Section 2.2 above, and must also:

a. where the information system(s) disclosed pursuant to 2.2(i) includes an Information Society Service, disclose, if applicable, that Cookies are used by the Participant and/or Third Parties to collect the Data Subject's PII via the Participant's Information Society Service, the particular types of Cookies used, and the purposes for which the PII collected by such Cookies is or will be used; and
b. where the Participant receives PII from a source other than the Data Subject, disclose from which source(s) (or categories of sources) the PII was obtained and, if applicable, that the PII was obtained from publicly accessible sources; and
c. where the Participant receives PII directly from the Data Subject, be made available to the Data Subject when the Participant first solicits or receives PII from the Data Subject, or as soon as practicable thereafter, and in any case before the Participant discloses such PII to any Third Party; and
d. where the Participant receives PII from a source other than the Data Subject, be made available to the Data Subject within a reasonable period (not more than thirty days) after receiving the PII.

2.4 Supplemental Privacy Notice Elements for Participants That Adhere to the EU-U.S. Privacy Shield Framework. Where the Participant is a U.S. entity and intends to certify its adherence to the EU-U.S. Privacy Shield Framework, that Participant's Privacy Notice must also:

a. include the Participant's commitment to adhere to the EU-U.S. Privacy Shield Framework; and
b. include the Participant's commitment to apply the Privacy Shield Principles to all PII it receives in reliance on the EU-U.S. Privacy Shield; and
c. provide a link to, or the website address for, the Privacy Shield List; and
d. disclose, if applicable, that the Participant has agreed to cooperate and comply with the dispute resolution panel established by the European Data Protection Authorities in addition to the VeraSafe Dispute Resolution Procedure; and
e. disclose the possibility, under certain conditions, for the Data Subject to invoke binding arbitration as described in the EU-U.S. Privacy Shield Framework; and
f. disclose the Participant's liability in cases of onward transfers to Third Parties.

2.5 Notice Requirements for Changes in Data Processing Procedures. Prior to making any material changes to its Privacy Notice, a Participant must:

a. notify VeraSafe of the proposed change(s); and
b. receive approval from VeraSafe prior to implementing the proposed change(s).

2.6 Subject to the applicable terms of any commercial agreement between VeraSafe and the Participant, the Participant must display the VeraSafe Privacy Seal on or within its Internet-based Information Society Services that are within the Scope of the Certification.

3. Basis For Processing PII.

3.1 Where the Participant is a Data Controller that Participant may Process PII

a. only on the basis of:
    1. the valid Consent of the Data Subject; or
    2. the performance of a contract to which the Data Subject is party; or
    3. the necessity to comply with a legal obligation to which the Data Controller is subject; or
    4. the protection of the Vital Interests of the Data Subject or of another natural person; or
    5. the legitimate interests pursued by the Participant or by a third party, except where such interests are outweighed by the interests or fundamental rights and freedoms of the Data Subject which require protection of PII, in particular where the Data Subject is under the age of thirteen; or
    6. the need to erase such PII where the Basis for Processing is otherwise obsolete; and
b. only for the specific, limited purposes disclosed in the Privacy Notice applicable to the collection of such PII and for other purposes which are compatible with those disclosed purposes, or:
    1. for other purposes pursuant to the further Consent of the Data Subject; or
    2. for those purposes strictly necessary to protect the Vital Interests of the Data Subject or of another natural person.

3.2 Notwithstanding the obligations of Section 3.1(a), where the Participant is a Data Controller, that Participant may only Process Sensitive PII on the basis of:

a. the valid Consent of the Data Subject; or
b. the protection of the Vital Interests of the Data Subject or of another natural person; or
c. the need to establish, exercise or defend a legal claim(s); or
d. the need to provide healthcare treatment, subject to all applicable laws regulating the privacy of PII concerning health; or
e. the need of the Participant to carry out its obligations or to exercise specific rights in the field of employment law; or
f. the need to erase such Sensitive PII where the Basis for Processing is otherwise obsolete.

3.3 Where the Participant is a Data Controller, that Participant must not condition the provision of goods or services on the Data Subject providing more PII than what is reasonably necessary for the purposes of Processing.

3.4 Where the Participant is a Data Processor, that Participant may not Process PII beyond as specified in the applicable data processing agreement implemented between the Participant and the Data Controller or between the Participant and another Data Processor acting on behalf of the Data Controller.

4. Onward Transfer.

4.1 Subject to the limitations of Section 3:

a. Where the Participant wishes to transfer or make available PII to an entity to which the Program Criteria do not apply, it may do so only where:
    1. the Data Subject has provided Consent to the proposed transfer, after having been informed of the risks of such transfers, such as those arising from the recipient's inadequate level of data protection; or
    2. the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller; or
    3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person; or
    4. the transfer is necessary for the establishment, exercise, or defense of important legal claims; or
    5. the transfer is necessary in order to protect the Vital Interests of the Data Subject or of another natural person, and where the Data Subject is physically or legally incapable of giving Consent; or
    6. the transfer is necessary to comply with lawful requests by public authorities, including national security or law enforcement requests.
b. Where none of the circumstances in Section 4.1(a) apply, the transfer shall be permissible if the Third Party recipient is obligated to provide at least the same level of data protection as is required by the Program Criteria (either by way of an enforceable written contract, Binding Corporate Rules as defined by the General Data Protection Regulation of the European Union, applicable law, or participation in a binding self-regulatory scheme).

4.2 Contract for Onward Transfers to Data Controllers. Subject to the limitations of Section 4.1, for a Participant to transfer PII to a Third Party Data Controller, the Participant must first, whenever reasonably possible under the circumstances:

a. enter into an enforceable written contract with the Third Party that restricts the Third Party to Processing the PII only for purposes compatible with the limited and specific purpose(s) for which the PII was originally collected, or with the further Consent of the Data Subject; and
b. ascertain that the Third Party is obligated to provide at least the same level of data protection as is required by the Program Criteria, either by way of an enforceable written contract, Binding Corporate Rules, applicable law, or participation in a binding self-regulatory scheme.

4.3 Contract for Onward Transfers to Data Processors. For a Participant to transfer PII to a Third Party Data Processor for Processing on behalf of the Participant, the Participant must, in addition to the obligations in Section 4.2:

a. ascertain that the Third Party employs only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality; and
b. take reasonable steps to confirm that the Third Party Processes the PII in a manner consistent with its obligations referred to in Section 4.2(b) and 4.3(a) above; and
c. obligate the Third Party to notify the Participant if the Third Party becomes unable to satisfy its obligations referred to in Section 4.2(b) and 4.3(a) above; and
d. take reasonable steps to stop and remediate unauthorized or noncompliant Processing by the Third Party, upon becoming aware of such Processing.

5. Choice.

5.1 Right to Object. Where the Participant is a Data Controller, Data Subjects have a right to object to the Participant's continued Processing of the Data Subject's PII where the Basis for Processing such PII is:

a. the Consent of the Data Subject;
b. the Vital Interests of the Data Subject or of another natural person;
c. the legitimate interests pursued by the Participant or by a third party, except in cases where the Participant can articulate that such Processing is lawful, done for explicitly specified and limited purposes, and is based on real and present legitimate interest(s), and that such interest(s) pursued by the Participant or by a third party outweigh the legitimate interests, rights, and freedoms of the Data Subject.

5.2 Notwithstanding the foregoing, where the Participant is a Data Controller and Processes PII for the purpose of direct marketing, the Data Subject shall have the unalienable right to object to such Processing without paying any fee. Where an objection is made by a Data Subject in accordance with this Section, the Participant may no longer Process the Data Subject's PII for such direct marketing purposes.

5.3 Where an objection is made by a Data Subject in accordance with Section 5.1 points (a) through (c), the Participant in question may no longer rely on the demurred Basis for Processing, and if no other Basis for Processing exists, the Participant may no longer Process such PII except as strictly necessary to comply with and implement the objection of the Data Subject.

5.4 Where the Participant is a Data Controller and Processes PII on the potentially objectable bases identified in Section 5.1 points (a) through (c), that Participant must provide Data Subjects one or more easy to use, conspicuous, readily available, and affordable means to object to such Processing of their PII.

5.5 The Data Subject's right to object, as established by this Section, is subject to reasonable limits, such as to allow the Participant the opportunity to authenticate the identity of the Data Subject, and to allow the Participant a reasonable amount of time to implement the Data Subject's wishes.

5.6 Where the Participant is a Data Controller, that Participant is responsible for ensuring the implementation of the Data Subject's wishes so exercised under this Section, including in the information systems of the Data Processors engaged by the Participant, unless doing so is not reasonably possible, would require disproportional effort, or where such responsibility is formally assigned to a third party that is, along with the Participant, a joint Data Controller for the Data Subject's PII.

6. Access.

6.1 Right of Access to and Correction of PII. Where the Participant is a Data Controller, Data Subjects have a right to:

a. obtain from the Participant confirmation of whether or not the Participant is Processing the Data Subject's PII; and
b. have communicated to them any such PII in a format that would be intelligible to a reasonable person, with regard given to, in particular, the age of the Data Subject; and
c. be told the source(s) from which the Participant obtained their PII, or any pertinent, available information as to the source of the PII; and
d. be told the Third Parties, or categories of Third Parties, to whom the Participant has disclosed or intends to disclose their PII; and
e. be told the purposes for which their PII has been or will be Processed, either by the Participant or any Third Party acting as the Participant's Data Processor; and
f. have their PII corrected or amended where it is inaccurate or incomplete.

6.2 Right to Erasure. Where the Participant is a Data Controller, Data Subjects have a right to obtain the erasure of their PII:

a. in cases where such PII is incorrect; or
b. where the Participant's Processing of such PII has materially violated the Program Criteria, applicable law(s), or applicable self-regulatory obligations; or
c. where the PII is no longer necessary for the purpose(s) of Processing or there is no longer a valid Basis for Processing; or
d. where the PII is collected via an Information Society Service and the Data Subject is under the age of thirteen.

6.3 Where the Participant is a Data Controller and the Participant has made a Data Subject's PII public, the Data Subject has the right to request that the Participant take all reasonable steps, including technical measures, to inform Third Parties which are Processing such PII, of the Data Subject's request to erase any copy or replication (and hyperlinks thereto) of such PII.

a. Where the Participant has authorized a Third Party publication of PII, the Participant shall remain responsible for that publication.

6.4 Limitations of the Right of Access, Correction, and Erasure.

a. Where the Participant is a Data Controller, that Participant must, at no charge to the Data Subject, implement the Data Subject's wishes so exercised under this Section 6, except:
    1. where the burden or expense of implementation would be overwhelmingly disproportionate to the risks to the Data Subject's privacy in the case in question; or
    2. where the Data Subject's PII cannot reasonably be separated from confidential commercial information; or
    3. where the implementation would interfere with the execution or enforcement of the law or with private causes of action, including the prevention, investigation, or detection of criminal offenses or the right to a fair trial; or
    4. where the legitimate rights or important interests of others would be violated; or
    5. where the implementation would breach a legal or other professional privilege or obligation to which the Participant is subject; or
    6. where the Data Subject's requests are vexatious or manifestly excessive, due in particular to their frequent or repetitive nature; or
    7. where the Processing of such PII is strictly necessary for historical, statistical, or scientific research purposes.
b. If a Participant determines that a Data Subject's right of access, correction, or erasure should be limited in any particular instance, the Participant must respond to the Data Subject with an explanation of why the Participant has made such a determination and provide information as to where the Data Subject can lodge further inquiries.

6.5 Where the Participant is a Data Controller, that Participant must provide Data Subjects one or more easy to use, conspicuous, readily available, and affordable means to exercise their rights under this Section.

6.6 Participants must confirm the identity of persons attempting to exercise rights under this Section, and only implement a Data Subject's wishes so exercised under this Section where the identity of such Data Subject has been adequately confirmed by the Participant.

6.7 Where the Participant is a Data Controller, that Participant is responsible for implementing the Data Subject's wishes so exercised under this Section, including in the systems of the Data Processors engaged by the Participant, unless doing so is not reasonably possible or would require a level of effort that is overwhelmingly disproportionate to the risks to the Data Subject's privacy in the case in question.

7. Data Security.

7.1 Within the Scope of the Certification, Participants must comply with the requirements of this Section.

7.2 Identify.

a. **Asset Management.** [ID.AM]
    1. Maintain an inventory of the hardcopy and electronic records and the electronic devices and storage media that the Participant uses to Process PII.
    2. Identify and appoint one or more natural persons who are responsible for the development and implementation of the data security policies and procedures required by the Program Criteria.

b. **Business Environment.** [ID.BE] (Reserved)

c. **Governance.** [ID.GV]
    1. Implement and maintain a high-level data security policy.

d. **Risk Assessment.** [ID.RA]
    1. If the Participant's workforce is comprised of 250 or more full-time equivalent employees, conduct an accurate and thorough assessment of the potential risks to the confidentiality, integrity, and availability of PII it Processes. Such assessment must:
        I. identify critical assets; and
        II. identify threats and vulnerabilities to those critical assets; and
        III. result in a formal, documented analysis of risk; and
        IV. be conducted based on established frameworks or methodologies such as NIST SP 800-30, ISO 27005, FAIR, or OCTAVE.

e. **Risk Management Strategy.** [ID.RM]
    1. Implement data security controls that ensure an appropriate level of confidentiality, integrity, and availability for the PII that the Participant Processes. The Program Criteria set a baseline of required data security controls; however, additional data security controls may be needed to establish an appropriate level of data security under a Participant's circumstances. In determining what is appropriate under the circumstances, regard should be given to the sensitivity of the PII, the purposes of Processing, the risks to the rights and freedoms of the Data Subject(s) that arise from such Processing, the cost of implementation and maintenance of such additional controls, and the consensus of professional opinion in the field of data security.

7.3 Protect.

a. **Access Control.** [PR.AC]
    1. Implement and maintain procedures to control and validate a person's physical and logical access to the Secured Facility(s), the information system(s), and the PII therein based on role or function, including visitor control.
        I. All users of Participant's information systems must be individually identified and authenticated.
        II. Restrict logical access to all Workstations, and administrator and non-consumer functions in other IT Systems, with a strong password known only to authorized users, whenever reasonably practicable.
        III. Implement and maintain appropriate entry controls to reasonably prevent unauthorized persons from physically accessing the Secured Facility(s). Such controls may include using locks and keys, badges and badge readers, key fobs, et cetera, as appropriate given the risks to the rights and freedoms of the Data Subjects presented by the Processing.
        IV. Require visitors to sign-in, wear a plainly visible "Guest" ID badge, and be escorted by an authorized individual at all times in the Secured Facility(s).

2. Implement and maintain policies and procedures for terminating access to the Secured Facility(s), the information systems, and the PII therein when an employee or contractor is separated from the Participant or when such access is no longer justifiable.
    I. Such policies must require that all of the Participant's physical authentication methods are either returned by such employees and contractors, or are deactivated.
3. Implement and maintain policies and procedures to authenticate and verify the identity of a user before granting the user's request to modify any authentication credential, such as resetting a password.
4. Implement and maintain policies and procedures to correctly authenticate and verify the identity of Data Subjects before granting such Data Subjects' requests to exercise rights with regards to PII Processed by Participant.
    I. Participant must not rely on fewer than two unique identifiers in authenticating such Data Subjects.
5. Implement and maintain policies and procedures to limit employees' and contractors' access to the Secured Facility(s), the information systems, and the PII therein to those natural persons with an identified, legitimate need for such access, incorporating the principle of least privilege.
    I. Regularly audit such privileged access rights (at least twice per year).

b. **Awareness and Training.** [PR.AT]
    1. Implement and maintain a data-security-training-program for all employees within the Scope of the Certification.
    2. Implement and maintain an ongoing data-security-awareness-program for all employees within the Scope of the Certification.
    3. Implement and maintain procedures for creating, changing, and safeguarding IT System passwords.
    4. Implement and maintain policies and procedures to mitigate risks that arise from unintentional insider threats.

c. **Data Security.** [PR.DS]
    1. Secure the transmission of PII and authentication information over non-private networks with strong cryptography and security protocols (such as recent Transportation Layer Security protocols) if the inappropriate use or disclosure of that data could cause financial, physical, or reputational harm to a Data Subject.
        I. Secure the transmission of PII and authentication information over wireless networks with strong cryptography and security protocols.
    2. Maintain (and implement as needed) procedures for securely disposing of PII when the Basis of Processing becomes obsolete.
    3. Implement and maintain policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical and technical attributes surrounding a specific Workstation or class of Workstations. Such policies and procedures must, at minimum:
        I. prohibit those software applications or categories of software applications that are likely to introduce a critical vulnerability, from being used or installed on the Workstations; and
        II. prohibit operating systems with unauthorized modifications (including rooted or jailbroken operating systems) from being used or installed on Workstations; and
        III. require users to re-authenticate to reactivate Workstations that have been idle for more than 15 minutes.
    4. Implement and maintain policies to regulate the removal of storage media containing PII from within the Secured Facility(s). Whenever reasonably practicable, such policies must:
        I. prohibit the removal of electronic storage media containing PII from within the Secured Facility(s), except for the occasional removal of PII done not on a large scale, or if such PII is encrypted with strong cryptography; and

II. prohibit the removal of PII in hardcopy from within the Secured Facility(s), except if such PII is reasonably physically secured when outside of the Secured Facility(s).

5. Implement and maintain policies and procedures to require that whole disc encryption, container-level encryption, or file-level encryption be used in portable Workstations and portable mass storage media, as appropriate, to secure PII and authentication information contained on those devices. In all such cases, the encryption must be cryptographically strong.
6. Implement and maintain policies to require that Workstations, storage media containing PII, and authentication information be physically secured when not in use, both inside and outside of the Secured Facility(s).
7. Implement and maintain appropriate technical controls to prevent, detect, and correct data integrity violations in IT Systems.
    I. Such controls may include checksums, mirroring, ECC memory, RAID parity, and file integrity monitoring tools.
8. Implement and maintain policies, whenever possible, to prohibit the use of PII for information system testing or development purposes.

d. **Information Protection Processes and Procedures.** [PR.IP]
    1. Implement and maintain policies and procedures to ensure that vendor-supplied default passwords and other authentication parameters in IT System(s) are changed, removed, or disabled.
    2. Implement and maintain a binding confidentiality agreement with employees who are within the Scope of the Certification.
    3. Implement and maintain policies to apply appropriate sanctions against employees who fail to adhere to the Participant's documented data security policies and procedures.
    4. Implement and maintain procedures to create and maintain retrievable exact copies of PII that the Participant stores or otherwise maintains.
    5. Implement and maintain appropriate environmental controls to protect the integrity and availability of mission critical information systems and PII that the Participant stores or otherwise maintains.
        I. Such controls may include emergency power supplies, emergency lighting, fire protection and suppression equipment, temperature and humidity controls, and measures to prevent water damage.
    6. Implement and maintain policies and procedures to ensure the removal of PII from storage media before such media are made available for re-use by the Participant.
    7. Implement and maintain policies and procedures to ensure the secure disposal of the media on which PII is or has been stored.
    8. Implement and maintain policies and procedures to detect technical security vulnerabilities in the IT Systems.

e. **Maintenance.** [PR.MA]
    1. Implement and maintain policies and procedures to patch exploitable and high severity security vulnerabilities that exist in IT Systems expeditiously after the discovery of such vulnerabilities.
        I. Such policies and procedures must require that vendor-supplied patches for exploitable and high severity IT System vulnerabilities be tested and applied to the affected IT Systems (or the vulnerability otherwise mitigated) within sixty days of the date on which the vendor released the patch.
    2. Implement and maintain policies and procedures to prohibit the use of deprecated software that is no longer updated by the author.

f. **Protective Technology.** [PR.PT]
    1. Limit repeated logical access attempts to IT System(s) by automatically locking out the user ID after not more than six consecutive failed access attempts.
        I. Set the lockout duration to a minimum of thirty minutes or until an administrator re-enables the user ID.

2. Implement a functional firewall and maintain its configuration to protect the IT Systems from untrusted networks and untrusted traffic.

7.4 Detect.

a. **Anomalies and Events.** [DE.AE]
   1. Establish a baseline of network operations and expected data flows.
   2. Analyze suspected Security Incidents to understand attack targets and methods.

b. **Security Continuous Monitoring.** [DE.CM]
   1. Implement and maintain policies and procedures to monitor the Secured Facility(s) and the IT Systems to detect Security Incidents and associated activity.
      I. Implement and maintain hardware, software, and/or procedural mechanisms to record and monitor technical activity in the IT Systems.
      II. Implement and maintain mechanisms to monitor physical activity in the Secured Facility(s), including the physical activity of contractors and visitors.
   2. Deploy antivirus software on all IT Systems that are commonly affected by malicious software. Such antivirus software must:
      I. be regularly, frequently updated; and
      II. automatically scan the IT System(s) where it is deployed; and
      III. not be disabled on the IT System(s) where it is deployed.

c. **Detection Processes.** [DE.DP] (Reserved)

7.5 Respond.

a. **Response Planning.** [RS.RP]
   1. Implement and maintain policies and procedures to respond to suspected or known Security Incidents.
   2. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that physically damages the Secured Facility(s) or the information system(s).
      I. Maintain (and implement as needed) procedures to ensure the continuation of those procedures that are necessary to protect the security of PII, while operating during an emergency.
      II. Maintain (and implement as needed) procedures for accessing PII during an emergency.

b. **Data Breach Notification.** [RS.CO]
   1. Where the Participant is a Data Controller, for any Data Breach in the Scope of the Certification, including in the information systems of the Participant's Data Processors and subprocessors, that Participant must transmit the information described in Section 7.5(b)(2) (a "Notice of Data Breach") to competent law enforcement agency(ies) and affected Data Subjects without delay and promptly after becoming aware of each such Data Breach, or do otherwise as required by law.
      I. Participant must promptly transmit its Notice of Data Breach to the competent law enforcement agency(ies), no later than seventy-two hours after becoming aware of such Data Breach.
      II. Unless a longer timeframe is officially requested by a competent law enforcement agency, the Participant must transmit its Notice of Data Breach to the Data Subjects no later than ten days after becoming aware of such Data Breach.
         A. Participant must provide its Notice of Data Breach to affected Data Subjects by way of its usual means of communicating with the Data Subjects, along with other means, if necessary.

B. If performing the obligation of 7.5(a)(1)II would require a disproportionate effort (for example, costing the Participant more than the lesser of ten percent of global turnover or $250,000 USD) the Participant may satisfy the obligation of 7.5(a)(1)II by making a public notification or similar measure whereby the Data Subjects are notified in an equally effective manner.

2. Unless otherwise required by applicable law, Participant's Notice of Data Breach must:
   I. be titled "Notice of Data Breach"; and
   II. disclose that a Data Breach occurred; and
   III. disclose the categories of PII that were disclosed in the Data Breach; and
   IV. disclose, if available, the approximate number of records that were exposed in the Data Breach; and
   V. disclose, if available, the approximate number of Data Subjects affected by the Data Breach; and
   VI. disclose when the Data Breach occurred; and
   VII. disclose what steps Data Subjects can take to protect themselves; and
   VIII. disclose likely consequences of the Data Breach; and
   IX. disclose the actions the Participant is taking regarding the Data Breach including the steps the Participant is taking to reduce the risk of a repeated or sustained Data Breach; and
   X. disclose the name and contact information of a representative of the Participant who can provide additional information regarding the Data Breach;
   XI. be written in the language(s) in which the Participant usually conducts its affairs; and
   XII. be provided in written form (which may be electronic), using clear language that a reasonable person would comprehend.
3. Where the Participant is a Data Processor, that Participant must transmit its Notice of Data Breach to the Data Controller(s) within 72 hours of becoming aware of each such Data Breach.
4. The Participant must act immediately, without undue delay, to patch any unmitigated exploitable IT security vulnerabilities and reduce the risk of a repeat or sustained Data Breach upon becoming aware of a Data Breach.
5. Participants must notify VeraSafe of the occurrence of a Data Breach no later than ten days from the date of discovery of the Data Breach unless a longer timeframe is officially requested by a competent law enforcement agency.

c. **Analysis.** [RS.AN]
   1. Implement and maintain policies and procedures to document Security Incidents and their outcomes.
d. **Mitigation.** [RS.MI]
   1. Implement and maintain policies and procedures to mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Participant.
e. **Improvements.** [RS.IM]
   1. Update policies and procedures based on lessons learned.

7.6 Recover.

a. **Recovery Planning.** [RC.RP]
   1. Maintain (and implement when needed) procedures to restore any unintentionally lost PII.
b. **Improvements.** [RC.IM] (Reserved)
c. **Communications.** [RC.CO] (Reserved)

8. Data Quality.

8.1 Where the Participant is a Data Controller, that Participant must take all reasonable steps to ensure that, with regard to the risks to the rights and freedoms of the Data Subject(s), PII it Processes is sufficiently reliable, accurate, complete, and current and that PII that are inaccurate are erased or rectified without unreasonable delay.

9. Privacy By Default.

9.1 Where the Participant is a Data Controller, that Participant must ensure that, by default, the PII it Processes is not made accessible, without the Data Subject's intervention, to an indefinite number of natural or legal persons.

10. Privacy Of Children.

10.1 Where the Participant is a Data Controller, that Participant must, where the Participant's Scope of the Certification includes Information Society Services:

a. ensure that the Information Society Service is not be directed at or intended for use by Data Subjects under the age of thirteen ("U13"); or
b. provide notice to parents or legal guardians of U13 ("Parent(s)") and obtain verifiable parental consent, such as in the form of a consent agreement signed by the Parent and returned to the Participant before Processing the PII of U13; and
c. give Parent(s) the opportunity to terminate such consent agreement at any time; and
d. give Parent(s) the choice of consenting to the Participant's internal Processing of their U13's PII, while prohibiting the Participant from disclosing that PII to a Third Party Data Controller (unless such disclosure is strictly necessary for the purpose(s) of Processing, in which case this must be made clear to Parents); and
e. enable Parent(s) to exercise the rights described in Sections 5 and 6 on behalf of their U13.
10.2 Where the Participant is a Data Controller, and the Participant becomes aware that it Processes the PII of a U13 without complying with Section 10.1(b)-(e), that Participant must securely dispose of such PII.

11. Commercial Email Communication.

11.1 Where the Participant is a Data Controller, and Processes PII for the purpose of sending Commercial Email Messages:

a. such Commercial Email Messages must include the Participant's valid postal address which can be a current street address, a post office box registered with the U.S. Postal Service, a private mailbox registered with a commercial mail receiving agency established under U.S. Postal Service regulations or, for Participants whose principal office(s) are located outside of the U.S., a valid and current post office box registered with the local governmental authority responsible for postal matters; and
b. such Commercial Email Messages must include a clear and conspicuous, functioning and free unsubscribe mechanism. Such unsubscribe mechanism must not require a Data Subject to give the Participant any PII beyond an email address, or make a Data Subject take any step other than sending a reply email or visiting a single page on a website as a condition for honoring an unsubscribe request. Participant must implement the Data Subject's unsubscribe request within ten business days of receipt of such a request.
    1. An unsubscribe mechanism is not required for Relationship Messages and a Participant may continue to send Relationship Messages after a Data Subject unsubscribes from Commercial Email Messages provided that the Data Subject continues a business or employment relationship with the Participant.

11.2 If a Data Subject has unsubscribed to the Participant's Commercial Email Messages, the Participant must not transfer that Data Subject's email address to any Third Parties for their direct marketing use.

12. Recourse and Enforcement.

12.1 Compliance Verification.

a. Participants must retain the records related to their compliance with the Program Criteria for at least six years from the date on which a record was created, or was last in effect, whichever is later.
b. Participants must regularly review their compliance with the applicable Privacy Notice(s) and these Program Criteria, and take remedial action, as appropriate, to ensure their ongoing compliance therewith.
c. Each Participant shall be subject to, and cooperate with, the Verification Process at least annually to verify its ongoing compliance with these Program Criteria.
d. The Verification Process can be re-initiated by VeraSafe at any time at VeraSafe's discretion.

12.2 Recourse.

a. Where the Participant is a Data Controller, that Participant must respond to data protection related inquiries or complaints it receives from Data Subjects within thirty days of receipt by the Participant.
b. Participants must cooperate with VeraSafe's efforts to investigate complaints pertaining to such Participant, that are determined to be valid and within the scope of these Program Criteria.
    1. Participants must cooperate and comply with the Procedure applicable to any such complaints.

12.3 Accountability.

a. In the event VeraSafe reasonably believes that a Participant has violated these Program Criteria or the applicable Master License and Services Agreement between VeraSafe and the Participant in a material way, such Participant's good standing in the Program may be suspended ("Program Suspension") by VeraSafe.
    1. In such circumstance, VeraSafe shall provide the suspended Participant with a description of the violation(s) and any remedial actions that VeraSafe will require the Participant to take during the Program Suspension period ("Program Suspension Obligations").
    2. Participant's participation in the Program shall be considered to be suspended immediately upon receiving notice to such effect from VeraSafe.
b. **Program Suspension Obligations.**
    1. Program Suspension Obligations may include, but are not limited to:
        I. implementation of additional data protection controls beyond those specified in the Program Criteria; and
        II. cooperation with additional compliance monitoring by VeraSafe; and
        III. payment to VeraSafe as compensation for VeraSafe's additional compliance monitoring activities.
    2. Participants must comply with all Program Suspension Obligations within forty-five days of receiving the suspension notice, unless a longer duration is mutually agreed upon between VeraSafe and the Participant.
    3. During the Program Suspension period, Participant's suspended status may be indicated via its VeraSafe instant verification page hosted by VeraSafe, and VeraSafe may revoke the Participant's license to display the VeraSafe Privacy Seal(s).
c. **Exiting Program Suspension.**
    1. Program Suspension shall last until such time as the Participant has corrected the material violation(s) to VeraSafe's satisfaction.

2. If the Participant has not rectified the material violation(s) by the end of the Program Suspension period, VeraSafe will, in its discretion, either:
    I. extend the Program Suspension period; or
    II. determine that Participant has failed to comply with the Program Suspension Obligations and apply one or more Enforcement Actions (as defined in the Section 12.3(d)) against the Participant.

d. **Enforcement Actions.**
    1. Subject to the provisions of Section 12.3, VeraSafe may:
        I. terminate the Participant's participation in the Program(s) ("Termination"); and
            A. Participants that are Terminated will no longer be entitled to use, reproduce, or display any of the VeraSafe Privacy Seals and must immediately stop all use of any VeraSafe Privacy Seal; and
            B. Participant's participation in the Program shall be considered to be Terminated immediately upon receiving notice to such effect from VeraSafe; and
        II. notify the relevant regulatory enforcement authority in the Participant's jurisdiction in cases where the Terminated Participant's material violations are, in VeraSafe's judgment, repeated or intentionally negligent; and
        III. make publicly available, a notice of the Terminated Participant's material violation(s) in cases where such material violation(s), in VeraSafe's judgment, constitute an ongoing risk to the rights and freedoms of Data Subjects; ("Enforcement Actions").

13. Requirement For Neutrality.

13.1 A Participant must not have a direct or indirect business affiliation with VeraSafe, or with any employee of VeraSafe, that would prejudice the ability of VeraSafe to render a fair decision with respect to the certification of the Participant. Such affiliations include but are not limited to the Participant and VeraSafe being under common control such that the Participant can exert undue influence in VeraSafe.