VeraSafe Privacy Shield Dispute Resolution Program Annual Report 2019-2020

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

Contents

Executive Summary

This report covers the period from August 1, 2019 to July 31, 2020, which marked the fourth 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 GDPR 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 "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.

The Safe Harbor arrangement, the immediate precursor to the Privacy Shield Frameworks, was the transatlantic data transfer mechanism of choice from the early 2000's 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.

Schrems II Decision

On July 16, 2020, the Court of Justice of the European Union invalidated the Privacy Shield Framework as a valid data transfer mechanism for personal data transferred from the European Union to the United States. However, the Privacy Shield Frameworks remain a valid transfer mechanism for personal data transferred from Switzerland to the United States, and the Department of Commerce will continue to administer the Privacy Shield Program, including processing submissions for self-certification and recertification to the Privacy Shield Frameworks. Therefore, organizations enrolled in the Privacy Shield Framework must continue to comply with the Privacy Shield Principles. VeraSafe will continue to operate VeraSafe Dispute Resolution Program and the VeraSafe Privacy Program in compliance with the Privacy Shield Certification Principles and our applicable program criteria.

Statistical Overview for the 2019-2020 Reporting Period

Membership Statistics			
	VeraSafe Dispute Resolution Program (IRM)	VeraSafe Privacy Program (Verification)	Both Programs
Number of Member Organizations	133	28	28

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

Increase in False Membership Claims

During the 2019-2020 reporting period, VeraSafe observed an increase in the number of organizations falsely claiming to be a member of VeraSafe's Dispute Resolution Program in their privacy notices. In each case where VeraSafe discovered a false claim, VeraSafe sought to have these claims removed by the organization inappropriately claiming membership. As of the date of this report, VeraSafe has successfully ensured the removal of two of the three false claims. We continue to pursue remedies to ensure removal by the third.

	VeraSafe Dispute Resolution Program (IRM)	VeraSafe Privacy Program (Verification)
Number of False Membership Claims	3	0

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 ("Participant") can easily do so at https://verasafe.com/public-resources/dispute-resolution/submit-dispute/

VeraSafe Dispute Resolution Services are always provided free of charge to data subject complainants ("Complainant").

In its fourth 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 fourth year of operation. Since 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.

To avoid an actual or potential conflict of interest in situations where VeraSafe provides a Participant with both verification services and dispute resolution services, VeraSafe screens members of its team from participating in both verification services and dispute resolution services for the same Participant, and VeraSafe further restricts access to Participant data for each service to VeraSafe team members responsible for the provision of that service.

Participation Requirements

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

In engaging VeraSafe, 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 monetary penalties against a Participant for its failure to comply with the Privacy Shield Framework(s), the VeraSafe Privacy Program Certification Criteria (the "Program Criteria;" the full text of which is available on VeraSafe.com (https://verasafe.com/privacy-solutions/privacy-program-certification-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 monetary penalties 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 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://verasafe.com/public-resources/dispute-resolution/privacy-shield-dispute-resolution-procedure/; and
- 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://verasafe.com/public-resources/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 personally identifiable information ("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 (as described below); 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 ("Permitted 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 the Privacy Shield itself.

The result was the VeraSafe Program Criteria, the full text of which is available on VeraSafe.com (https://verasafe.com/privacy-solutions/privacy-program-certification-criteria/).

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

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

While the former 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 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 former 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 the GDPR, data subjects have a right to access their personal data with regard to all types of processing, not only data storage.

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.

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

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

An ambiguity that the former 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 Participants whether they are 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.

Conclusion

VeraSafe has set forth a data protection standard that incorporates the requirements of the Privacy Shield Frameworks, the views of the former Article 29 Working Party, and the NIST CSF. VeraSafe considers that upon successful completion of our Privacy Program assessment, organizations are particularly well-equipped to protect personal data and to safeguard 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.

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

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, CIPM
matt@verasafe.com
Managing Director

James Cormier, CIPP/E
Senior Counsel and SVP Professional Services and Legal
jim@verasafe.com

VeraSafe U.S.:

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

VeraSafe EU:

VeraSafe Czech Republic
Klimentská 46
Prague 11000
Czech Republic

EXHIBIT A

VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure

Last Updated: April 16, 2020

1. Introduction.

1.1. The VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure (the "Procedure") is provided and administered by VeraSafe, 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)"), that 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, (available at https://www.privacyshield.gov/EU-US-Framework) and the Enforcement Principle and FAQ 11 "Dispute Resolution and Enforcement" of the Safe Harbor Frameworks (available at https://2016.export.gov/safeharbor/eu/eg_main_018493.asp). 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 one or more allegation(s) of non-compliance with 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 filed with VeraSafe under the terms of the Procedure.

d. "Data Privacy Hearing" means the process described under Section 8 of the Procedure.

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 Framework.

g. "Participant" means a member, in good standing, 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 under the Procedure by the Parties or by VeraSafe.

j. "Settlement Agreement" means an agreement reached by the Parties that resolves the Complaint. To be effective, the terms of such agreement must be recorded in writing and signed by both Parties.

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 set forth at https://www.verasafe.com/privacy-services/certification-standard/ (such hyperlink may be revised and redirected from time to time).

3. General Terms and Eligibility.

3.1. Legal Representation. One or both Parties may choose to be represented by legal counsel at any stage of the Procedure. If either Party chooses to be represented, that party will notify VeraSafe, providing the name and contact information of the attorney who will be representing the Party. VeraSafe will then notify the other Party of the representation and the attorney's name and contact information.

3.2. No Payment Required. The Complainant is not required to pay any remuneration to VeraSafe in order to file a Complaint with the Procedure.

3.3. Eligible Complainant. For a Complainant to be eligible to file a Complaint, the Complainant must be:

a. at least thirteen years of age on the date the Complaint is filed under the Procedure and a Data Subject whose PII was exported from the EEA or Switzerland by or to a Participant; or

b. the parent or legal guardian of a Data Subject (1) who is under eighteen years of age at the time that the Complaint is filed with VeraSafe and (2) whose PII was exported from the EEA or Switzerland by or to a Participant.

3.4. Eligible Complaint. For a Complaint to be eligible under the Procedure, the Complaint must:

a. name a Participant 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;

b. not have been previously resolved or settled by court action, arbitration, or other form of dispute resolution;

c. be filed using the Procedure for the first time, except for Complaints (1) alleging a Participant's failure to comply with a previous Settlement Agreement or (2) being amended pursuant to Section 4.3; and

d. not seek remedies that are not Permitted Outcomes.

3.5. 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.

3.6. Complainant's Right to Appeal the Ineligibility Determination. The Complainant has the right to appeal VeraSafe's Ineligibility Determination within ten business days of being sent the Ineligibility Determination. If the Complainant can show a reasonable likelihood that VeraSafe made a material error in the Ineligibility Determination, VeraSafe shall duly re-examine the Complaint and make a final determination as to its eligibility. VeraSafe's determination shall be final after the appeal and no further appeal may be taken.

4. Complaint Filing Procedure.

4.1. 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 applicable privacy notice(s) entirely before filing a Complaint with VeraSafe. If VeraSafe determines, in its sole discretion, that Complainant did not make a good faith effort to resolve the dispute before filing a Complaint, VeraSafe shall require the Complainant to try to resolve the Complaint directly with the Participant and shall advise the Complainant that he or she may re-file the Complaint using the Procedure, as outlined herein, if the attempt to resolve the Complaint with the Participant does not yield satisfactory results.

4.2. 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. include the fullest possible account of facts and events giving rise to the Complaint;

c. seek one or more of the Permitted Outcomes (see Section 5.1);

d. if any damages or harm is alleged, include specific details of the harm and/or damages (where applicable, quantification of monetary damages is preferred, but not required);

e. include valid contact information (mailing address, email address, and contact person) for the Complainant;

f. include consent to share the Complaint with the Participant;

g. include all available documentation to support the Complaint;

h. include a description of Complainant's good faith effort to resolve the dispute with the Participant, before filing 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.

4.3. Right to Correct Defective Complaint. Within ten business days of receiving the Complaint, VeraSafe will inform the Complainant if the Complaint fails to meet any of the requirements enumerated in Section 4.2 and will give the Complainant the opportunity to amend the Complaint to satisfy such requirement(s). As a matter of course, the Complainant will have two opportunities to amend the Complaint for failure to address any defects in the Complaint. Further opportunities to amend the Complaint to satisfy the requirements of Section 4.2 shall be given solely at VeraSafe's discretion.

4.4. Medium for all Procedure Submissions.

a. Complaints must be initiated by: (i) submitting VeraSafe's online complaint form located at: https://www.verasafe.com/privacy-services/dispute-resolution/submit-dispute/; or (ii) by submitting the required information to VeraSafe via email (experts@verasafe.com) and including the following statement: "I represent and warrant that I have read, understand, and agree to be bound by the terms of the VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure".

b. VeraSafe shall provide all 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.

5. Permitted Outcomes.

5.1. 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 or Appellate Hearing during the Procedure, are limited to the non-exclusive remedies 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. the Participant to 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 any orders set forth by the Hearing Officer or Appeal Officer.

5.2. In order to ensure that any sanctions are sufficiently rigorous – in accordance with Supplemental Principle 11(e)(i) of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks – VeraSafe reserves the right to impose additional sanctions upon the Participant that are more severe than those sought by the Complainant in situations where VeraSafe determines that such requested sanctions are inadequate to ensure Participant's compliance with the Framework(s); provided, however, that the fulfillment of the Complainant's desired outcome(s) shall be satisfied, at minimum.

6. Complaint Response Procedure.

6.1. 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") with VeraSafe within twenty business days of Participant's receipt of the Complaint from VeraSafe. The Participant's Response must either:

a. defend the Participant's actions as permitted under the applicable 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) as determined by VeraSafe in its sole discretion.

6.2. Upon VeraSafe's receipt of the Participant's Response, VeraSafe will forward it to the Complainant.

6.3. Participant's Failure to Respond. If the Participant fails to file a timely Response, the failure to comply with the Procedure will be duly noted in the next Annual Procedure Report (as such term is defined in Section 15 of the Procedure) and VeraSafe shall refer the matter to the appropriate government agency in accordance with Section 14 of the Procedure.

7. Consultative Mediation.

7.1. Mediation Teleconference. If the Complainant is not satisfied by the Participant's Response to the Complaint, and desires to continue with the Procedure, the Complainant must 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. 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 with the assistance of an approved mediator under the requirements set forth herein.

a. If the Complainant is satisfied by the Participant's Response to the Complaint, the Complainant shall notify VeraSafe in writing that the Complaint has been resolved.

b. If VeraSafe receives notification from the Complainant that the Complainant is satisfied with the Participant's Response, or otherwise receives no request for a Mediation Teleconference from the Complainant within the timeframe specified in Section 7.1, VeraSafe shall close the Complaint with an outcome of "Closed by Default" and duly notify the Parties.

7.2. Mediation Teleconference Procedure. VeraSafe will provide and appoint a mediator to lead the Mediation Teleconference with a requisite knowledge of data privacy concepts and the issues involved in the Parties' dispute to lead the Mediation Teleconference (the "Mediator"). 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 business days before the date of the Mediation Teleconference.

a. **Possible Outcomes of the Mediation Teleconference.**

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 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 14.

III. **Mutual Settlement Agreement.** If the Parties reach an agreement during the Mediation Teleconference, VeraSafe will record the terms of the Settlement Agreement (as decided by the Parties) and notify both Parties in writing of those terms within five business days of the Mediation Teleconference.

IV. **No Settlement Reached.** If no Settlement Agreement is reached during the Mediation Teleconference, the Complainant must file with VeraSafe a request for a Data Privacy Hearing within ten business days of the Mediation Teleconference or 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 (the "Data Privacy Hearing Officer") will review the Complaint and all Procedure Submissions in a fair and impartial way and determine if the available evidence does, by a preponderance of the evidence, substantiate the alleged violation of the Framework(s) made in the Complaint.

8.2. Exchange of Briefs. The Complainant's request for a Data Privacy Hearing should include a detailed brief supporting the allegation(s) in the Complaint (attaching evidence, if appropriate). Upon receipt, VeraSafe will forward the brief to the Participant. The Participant shall provide a brief in rebuttal to VeraSafe (attaching evidence, if appropriate) within ten business days of receiving the Complainant's brief.

8.3. Data Privacy Hearing Officer.

a. The Data Privacy Hearing Officer shall: (i) hold a current Certified Information Privacy Professional or Certified Information Privacy Manager credential from the International Association of Privacy Professionals; (ii) hold a Juris Doctor degree from an American Bar Association accredited law school; or (iii) 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.

c. The Data Privacy Hearing Officer shall not be the same individual who served as the Mediator.

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 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. **Scheduling of Data Privacy Hearing**. VeraSafe will make a reasonable effort to schedule a teleconference for the Data Privacy Hearing with due regard for the schedules of the Parties and will notify the Parties of the scheduled time and date not less than fifteen business days before the date of the teleconference.

c. **Data Privacy Hearing Procedure**. The Parties shall appear telephonically at the hearing, where they will be allowed to present their arguments and evidence (although no new arguments or evidence not contained

in the Procedure Submissions will be allowed, unless good cause is shown as to why they were not included). Additionally, the Data Privacy Hearing Officer may ask questions of the Parties about their arguments and evidence.

d. **Hearing Decision and Burden of Proof.** The Data Privacy Hearing Officer shall, based on the Procedure Submissions and Data Privacy Hearing, decide if the available evidence does, by a preponderance of the evidence, substantiate the allegation(s) 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. **Sustained Complaints.** If, after weighing the arguments and evidence presented in the Procedure Submissions and Data Privacy Hearing, and in due consideration of the totality of the circumstances, the Data Privacy Hearing Officer determines that the available evidence does, by a preponderance of the evidence, substantiate the allegation(s) 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, after weighing the arguments and evidence presented in the Procedure Submissions and Data Privacy Hearing, and in due consideration of the totality of the circumstances, the Data Privacy Hearing Officer determines that the available evidence does not, by a preponderance of the evidence, substantiate the allegation(s) 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. Appeal of Data Privacy Hearing Outcome. 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 reasonably believes that VeraSafe or the Data Privacy Hearing Officer failed to adhere to the Procedure and such failure materially affected the Hearing Decision.

9.2. Exchange of Briefs. To be considered, the Complainant's appeal brief must include a detailed briefing of the alleged failure to adhere to the Procedure, as well as any supporting evidence. Upon receipt of the appeal brief, VeraSafe will forward the appeal brief to the Participant. The Participant must provide a brief in rebuttal (including any supporting evidence) to VeraSafe within ten business days of receiving the Complainant's appeal brief. The briefs are the "Appellate Procedure Submissions".

9.3. Appellate Hearing Officer. VeraSafe will appoint an impartial officer to administer the Appellate Hearing (the "Appellate Hearing Officer") using the eligibility criteria described in Section 8.3. The Appellate Hearing Officer will not be the same individual who served as the Mediator or the Data Privacy Hearing Officer.

9.4. Appellate Hearing Administration and Procedure.

a. **Consideration of Appeal.** The Appellate Hearing Officer will accept an appeal when the Appellate Procedure Submissions demonstrate that there is a reasonable likelihood that VeraSafe or the Data Privacy Hearing Officer failed to adhere to the Procedure and that such failure materially affected the Hearing Decision. If the Appellate Hearing Officer accepts the appeal, he or she will execute the Appellate Hearing Procedure. If the Appellate Hearing Officer declines to accept the appeal, he or she will provide a written explanation of the decision, which will be provided to Complainant and Participant.

    I. The Appellate Hearing Officer may request additional information or seek clarification from either Party regarding the Appellate Procedure Submissions, either when considering the Appeal or when carrying out the Appellate Hearing Procedure.

b. **Appellate Hearing Procedure.** The Appellate Hearing Officer will duly examine the Appellate Procedure Submissions, as well as the Procedure Submissions, and shall decide if the available evidence does, by a

preponderance of the evidence, substantiate the allegation(s) made in the Complaint and, if so, whether or not the alleged action or inaction of the Participant is in violation of the applicable Framework(s) (the "Hearing Decision").

I. **Sustained Complaints.** If, in due examination of the Appellate Procedure Submissions and Procedure Submissions, and in due consideration of the totality of the circumstances, the Appellate Hearing Officer determines that the available evidence does, by a preponderance of the evidence, substantiate the allegation(s) made in the Complaint, and that the action or inaction of the Participant does violate the applicable 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 Appellate Procedure Submissions and Procedure Submissions, and in due consideration of the totality of the circumstances, the Appellate Hearing officer determines that the available evidence does not, by a preponderance of the evidence, substantiate the allegation(s) 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. The Complaint will then be closed with an outcome of "Closed – Withdrawn" and the Parties duly notified.

11. Complainant's Noncompliance with the Procedure.

11.1. If the Complainant breaches any term(s) of the Procedure in a material way, during any stage of the process, VeraSafe has the right to close the Complaint, record an outcome of "Closed by Default," and the parties duly notified.

12. Language.

12.1. 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.

13. Participant's Performance Under a Settlement Agreement or Reparation Order.

13.1. VeraSafe shall monitor the Participant's compliance with any Settlement Agreements or Reparation Orders entered or issued under the Procedure.

13.2. When VeraSafe is satisfied with the Participant's performance regarding an applicable Settlement Agreement or Reparation Order entered or 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.

13.3. Participant's Non-Compliance. If Participant fails to comply with a Settlement Agreement or Reparation Order entered or 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 14.

14. Referral to Government Agencies.

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

a. the Participant refuses to comply with the Procedure in regard 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 Agreement or Reparation Order entered or issued under the Procedure within a reasonable time.

14.2. 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.

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

14.4. 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.

15. Public Reporting.

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

a. an executive summary, including the period covered in the Annual Procedure Report, the name of the Privacy Shield dispute resolution program (the "VeraSafe Privacy Shield and Safe Harbor Dispute Resolution Procedure") and any highlights from the period;

b. the number of organizations presently enrolled in the Procedure;

c. the number of organizations that receive VeraSafe's Privacy-Shield verification service, and the number of organizations that receive both the verification service and the dispute resolution service;

d. a description of how VeraSafe avoids any actual or potential conflicts of interest in situations when it provides an organization with both verification services and dispute resolution services;

e. a brief description of the types of Privacy Shield-related guidance that VeraSafe provides (e.g., online guidance for businesses and consumers, involvement in presentations and other public discussions);

f. a description of the types of Privacy Shield-related compliance activities that VeraSafe engages in (e.g., review methods used by VeraSafe as part of its Privacy Shield-related verification service, or other steps that VeraSafe takes to review and/or monitor organizations' privacy policies);

g. the requirements for participation in the Program, including the elements of any participation agreement;

h. a description of how a Complaint can be filed with the Procedure;

i. a description of the Procedure's Complaint eligibility requirements and its complaint review process, including how long it takes for Complaints to be processed and resolved and the range of potential remedies; and

j. statistics for Privacy Shield-related complaints during the reporting period, which shall include:

   I. the number of Privacy Shield-related complaints[4] received during the reporting year;

   II. the types of Privacy Shield-related complaints received;

   III. the dispute resolution quality measures for the Privacy Shield-related complaints received (e.g., the length of time taken to process those complaints); and

4 For purposes of the annual report, a Privacy Shield-related complaint is a complaint that meets the following criteria: 1) complainant is an EU or Swiss individual (i.e., individual submitting on his/her own behalf or on behalf of a minor of whom the individual is the parent or guardian); (2) complaint concerns an organization enrolled in the Procedure; (3) complaint concerns an organization participating in the Privacy Shield program; and (4) complaint alleges that an organization has violated the Privacy Shield Principles with respect to complainant's own personal data (i.e., individual's own personal data or personal data of the minor of whom the individual is the parent or guardian).

IV. the outcomes of the Privacy Shield-related complaints received, notably the number and types of remedies or sanctions imposed.

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

16. Confidentiality.

16.1. Other than the Hearing Decisions and except as noted in Sections 14 and 15, all Procedure Submissions, deliberations, meetings, proceedings, and writings of the Procedure shall be treated as confidential by VeraSafe.

16.2. 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).

17. LIMITATION OF LIABILITY.

17.1. 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: ANY MEDIATOR, HEARING OFFICER, VERASAFE, NOR ANY VERASAFE EMPLOYEE, BOARD MEMBER, COMPANY OFFICER, OR INDEPENDENT CONTRACTOR UTILIZED BY VERASAFE IN THE PROCEDURE.

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

18. Interpretation.

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

19. Waiver of Subpoena.

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

20. Hold Harmless.

20.1. The Participant agrees to hold VeraSafe, its officers, agents, independent contractors, 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.

20.2. 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.

21. Relationship of the Parties.

21.1. 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.

21.2. 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.

22. Contact Information.

22.1. VeraSafe may be contacted using the contact information found at https://www.verasafe.com/about-verasafe/contact-us/.

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

22.3. 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.