



# VeraSafe DPF Dispute Resolution Program Annual Report 2023-2024

Contents

Executive Summary.....1

About the Data Privacy Frameworks .....1

    History of the Data Privacy Framework and its Antecedents.....1

    Pending Adequacy of the Swiss-U.S. Data Privacy Framework .....2

    About This Annual Report.....2

Statistical Overview for the Reporting Period .....2

    Membership.....2

    Eligible Disputes .....2

Conflicts of Interest.....3

VeraSafe’s Independent Recourse Mechanism Services .....3

VeraSafe’s Privacy Program, the GDPR, and Beyond .....3

Conclusion.....4

Contact VeraSafe .....5

EXHIBIT A.....6

EXHIBIT B.....7

## Executive Summary

This report covers the period from July 17, 2023 through July 16, 2024 (the “Reporting Period”).

VeraSafe’s Dispute Resolution Program is offered as a standalone service, and also as a component of two more comprehensive services – VeraSafe’s long-running Enterprise Privacy Program as well as its DPF Verification and Certification Program. Under each of these programs, VeraSafe performs outside compliance reviews to verify an organization’s compliance with the Data Privacy Frameworks.

Highlights from VeraSafe’s experience providing these services during the Reporting Period include receiving more than 20 complaint submissions, of which six were deemed eligible and processed in accordance with VeraSafe’s DPF Dispute Resolution Procedure.

## About the Data Privacy Frameworks

### History of the Data Privacy Framework and its Antecedents

The General Data Protection Regulation of the European Union (the “GDPR”) prohibits the transfer of personal data to countries outside the European Economic Area (“EEA”) whose laws do not offer a level of data protection essentially equivalent to those of the European Union (“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.

No such adequacy decision has been issued in respect of the United States itself, and so would-be transferors and transferees have seen a series of alternative data transfer mechanisms arise, fall out of favor, and be replaced.

On July 26, 2000, the European Commission issued an adequacy decision for the U.S.-EU Safe Harbor Framework, which remained the transatlantic data transfer mechanism of choice until October 6, 2015, when that adequacy decision was invalidated by the European Court of Justice.

On July 12, 2016, the European Commission issued an adequacy decision for the Safe Harbor Framework’s replacement, named the EU-U.S. Privacy Shield Framework. This met the same fate as its predecessor on July 16, 2020 at the hands of the Court of Justice of the European Union. However, that court’s decision did not relieve participants in the EU-U.S. Privacy Shield Framework of their obligations thereunder, and the U.S. Department of Commerce’s International Trade Administration continued to administer the Privacy Shield Program.

On July 10, 2023, the European Commission issued an adequacy decision in respect of a third-generation framework entitled the EU-U.S. Data Privacy Framework (the “EU-U.S. DPF”), and on October 12, 2023 an extension to the EU-U.S. DPF went into effect in respect of personal data transfers to the United States from the United Kingdom and Gibraltar (the “UK Extension”).

## Pending Adequacy of the Swiss-U.S. Data Privacy Framework

While there exists an analogous framework in respect of personal data transfers to the United States from Switzerland (the “Swiss-U.S. DPF”; together with the EU-U.S. DPF and the UK Extension, the “Data Privacy Frameworks”), as of the end of the Reporting Period adequacy regulations have not been issued by the relevant Swiss authorities. As a result, while eligible organizations in the United States may self-certify their compliance pursuant to the Swiss-U.S. DPF, personal data cannot be received in reliance on it until its adequacy is assessed.

## About This Annual Report

Most pertinent to this report, each organization participating in a Data Privacy Framework is required to provide an unbiased dispute resolution forum for individuals with privacy grievances against it. As it was under prior iterations of the Data Privacy Frameworks, this is known as an independent recourse mechanism (“IRM”).

VeraSafe is such a provider of IRM services, and it publishes this report annually in order to share an overview of its experience as a qualified IRM provider.

## Statistical Overview for the Reporting Period

### Membership

As of July 16, 2024:

- 28 organizations were members of either VeraSafe’s Privacy Program or VeraSafe’s DPF Verification and Certification Program, and were thereby also granted membership in VeraSafe’s Dispute Resolution Program;
- 160 organizations held membership in VeraSafe’s Dispute Resolution Program on a standalone basis; and
- in sum, 188 organizations were members of VeraSafe’s Dispute Resolution Program.

### Eligible Disputes

VeraSafe received 26 DPF Principles-related complaints during the Reporting Period, of which it determined six were eligible for resolution in accordance with its DPF Dispute Resolution Procedure described in the next section.

Of those six eligible complaints received during the Reporting Period, four have been definitively resolved as of the end of the Reporting Period and are summarized in Exhibit A hereto.

The relative lack of eligible complaints meets VeraSafe’s expectations particularly for its clients who are members of VeraSafe’s Privacy Program. Since VeraSafe’s Privacy Program exceeds the data protection requirements of the Data Privacy Frameworks, members achieve not only Data Privacy Framework compliance but also graduate from our assessments with a mature data

protection program that aligns with the high standards of European data protection law, which genuinely limits the opportunity for compliance issues to arise.

Similarly, members in VeraSafe's DPF Verification and Certification Program benefit from the same principles, approach, and assessment quality as the Privacy Program but within the narrower scope of the Data Privacy Frameworks.

## Conflicts of Interest

To avoid an actual or potential conflict of interest in situations where VeraSafe provides a client with both verification services and dispute resolution services, VeraSafe effectively screens members of its team from participating in both verification services and dispute resolution services for the same client.

## VeraSafe's Independent Recourse Mechanism Services

To fulfill its role as an IRM (whether on a standalone basis or as a part of the Privacy Program or DPF Verification and Certification Program), VeraSafe has created its DPF Dispute Resolution Procedure (the "Procedure," attached to this report as Exhibit B), which incorporates the Data Privacy Frameworks' IRM requirements into a broader, balanced dispute resolution process designed to address privacy complaints from data subjects in Europe and throughout the world. In the spirit of transparency, the full text of the Procedure is also publicly available at <https://verasafe.com/public-resources/dispute-resolution/dispute-resolution-procedure/>.

Data subjects who wish to submit a dispute concerning an organization that has selected VeraSafe as its IRM can do so easily, and at no cost to the data subject, by filling out a simple webform at <https://verasafe.com/public-resources/dispute-resolution/submit-dispute/>.

Potential complainants are advised that certain eligibility requirements must be met in order for a dispute submission to be treated as valid. For example, they must have made a good faith effort to resolve their dispute directly with VeraSafe's client before filing a complaint with VeraSafe. These requirements and other useful information are detailed in the Procedure; VeraSafe encourages all potential complainants to review the Procedure prior to filing a complaint with VeraSafe.

## VeraSafe's Privacy Program, 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 businesses. Rather than constrain the Privacy Program by basing it solely on the tenets of the Data Privacy Frameworks, VeraSafe has created a comprehensive, forward-looking privacy solution even more heavily aligned with the higher standards of the GDPR than the Data Privacy Frameworks themselves. The result is VeraSafe's "Program Criteria," available at <https://verasafe.com/privacy-solutions/privacy-program-certification-criteria/>.

VeraSafe’s Privacy Program goes beyond a strict interpretation of the Data Privacy Frameworks and attempts to bridge the gap between them and the GDPR in multiple ways, including by:

- incorporating existing technological and informational security standards like the U.S. National Institute of Standards and Technology’s Framework for Improving Critical Infrastructure Cybersecurity into the Program Criteria, to ensure that each Privacy Program assessment is conducted with exceptional rigor and attention to detail;
- aligning the Program Criteria with the access principles of the GDPR to better address the GDPR’s definition of “processing,” which is more expansive than the Data Privacy Frameworks’ focus on data storage; and
- actively providing privacy and data security training to clients’ workforces, as well as providing clients with the resources to conduct and track the progress of training in-house on an ongoing basis through PrivacyTrain, our proprietary library of privacy and information security learning content.

## Conclusion

VeraSafe is a trusted provider of data protection services to organizations in the United States and throughout the world. Its Privacy Program is a comprehensive set of privacy assessment and compliance solutions that not only incorporates the requirements of the Data Privacy Frameworks but also prepares participating organizations for privacy laws and frameworks further afield. Its DPF Verification and Certification Program does the same for clients whose focus is limited to the Data Privacy Frameworks. And its DPF Dispute Resolution Program, which is included in those two programs and offered on a standalone basis, provides an effective independent recourse mechanism for the benefit of clients and their data subjects.

VeraSafe remains confident that its clients and their data subjects will experience continued success with the Data Privacy Frameworks as their transatlantic data transfer mechanisms.

*[ Remainder of Page Intentionally Left Blank ]*

## 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, FIP  
Managing Director  
[matt@verasafe.com](mailto:matt@verasafe.com)

### VeraSafe U.S.:

VeraSafe  
100 M Street S.E., Suite 600  
Washington, D.C. 20003  
USA

### VeraSafe EU:

VeraSafe Czech Republic  
Klimentská 46  
Prague 11000 Czech Republic

# EXHIBIT A

## Summary of Eligible Disputes That Were Both Initiated and Resolved During the Reporting Period

### **Complaint No. 1:** August 19, 2023 – October 13, 2023

Complainant, located in the United Kingdom, attempted to make a purchase from Participant’s American website using a foreign credit card. Participant declined the transaction. Complainant claimed their privacy was violated by Participant knowing the card’s country of issuance and so desired the closure of their account with Participant.

*Resolution:* Participant attempted to facilitate the request but Complainant stopped communicating. After following up with Complainant, VeraSafe closed the dispute.

### **Complaint No. 2:** September 21, 2023 – January 29, 2024

Participant, located in Europe, transferred personal data to and sold products on Participant’s American website but closed their account. After realizing their products nevertheless remained for sale, Complainant desired that Participant confirm the account’s deletion and investigate whether Complainant’s account or personal information had been compromised.

*Resolution:* Participant determined Complainant had accidentally opened a second account in another country and confirmed the deletion of both accounts to Complainant’s satisfaction.

### **Complaint No. 3:** February 16, 2024 – April 10, 2024

Complainant, located in Europe, transferred personal data to and maintained an account on Participant’s American website. Complainant claimed Participant was misusing their personal information associated with that account and so desired its closure.

*Resolution:* Participant confirmed the deletion of the account to Complainant’s satisfaction.

### **Complaint No. 4:** April 5, 2024 – April 29, 2024

Complainant, located in Europe, claimed to have transferred personal data in connection with a GDPR data subject access request to Participant, located in the United States, and not received a response. Complainant desired that Participant respond to that initial request.

*Resolution:* Participant responded to Complainant confirming their request had been escalated to the data controller, following which Complainant withdrew their complaint.



# EXHIBIT B

## VeraSafe Data Privacy Framework (DPF) Dispute Resolution Procedure

Last Updated: July 19, 2023

### 1. Introduction

**1.1.** The VeraSafe Data Privacy Framework (DPF) 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 Data Privacy Framework (DPF) Dispute Resolution Program (the “Program(s)”), that is also subject to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and as applicable, the UK Extension to the EU-U.S.DPF, and/or the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) (together, the “Data Privacy Framework”), 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 Data Privacy Framework (available at <https://www.dataprivacyframework.gov/>), 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 one or more allegation(s) of non-compliance with the Data Privacy Framework, 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 Data Privacy Framework, 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 Data Privacy Framework 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-solutions/privacy-program-certification-criteria/> (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, UK (or Gibraltar), 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, UK (or Gibraltar), 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 Data Privacy Framework, 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/public-resources/dispute-resolution/submit-dispute/> or (ii) by submitting the required information to VeraSafe via email ([experts@verasafe.com](mailto: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 Data Privacy Framework 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 Data Privacy Framework – 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 reexamine 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 dispute resolution program (the “VeraSafe Data Privacy Framework 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 Data Privacy Framework 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 Data Privacy Framework-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 Data Privacy Framework-related compliance activities that VeraSafe engages in (e.g., review methods used by VeraSafe as part of its Data Privacy Framework-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 Data Privacy Framework-related complaints during the reporting period, which shall include:
  - I. the number Data Privacy Framework-related complaints received during the reporting year;
  - II. the types of Data Privacy Framework-related complaints received;
  - III. the dispute resolution quality measures for the Data Privacy Framework-related complaints received (e.g., the length of time taken to process those complaints); and
  - IV. the outcomes of the Data Privacy Framework-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-us/contact-us/>.

**22.2.** The International Trade Administration of the U.S. Department of Commerce may be contacted via the website <https://www.dataprivacyframework.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>.