TrustArc

Independent Recourse Mechanism Annual Report

Reporting Period: August 1, 2022 through July 31, 2023

 | US +1 415520 3490 | EU +44 (0)203.078.6495 | www.trustarc.com

EXECUTIVE SUMMARY

This annual report of TrustArc Inc summarizes the Privacy Shield services in its seventh year of operation for the reporting period August 1, 2022 through July 31, 2023. TrustArc operates two core services under its TRUSTe brand. These services include:

An Independent Recourse Mechanism:
TRUSTe Dispute Resolution

Privacy Shield Compliance Verification

Participation in the TrustArc Privacy Shield services during this reporting period included:

123	219	27	186	25
TRUSTe Dispute Resolution Only	**EU-U.S. Privacy Shield Verification and Dispute Resolution**	**EU-U.S. Privacy Shield Verification HR Data Only**	**Swiss-U.S. Privacy Shield Verification and Dispute Resolution**	**Swiss-U.S. Privacy Shield Verification HR Data Only**

Among the participants in the Privacy Shield services during the period,73 transitioned to inactive status on the Privacy Shield list during the period, comprising 47 of the Verification and Dispute Resolution participants, and 26 of the Dispute Resolution-only participants.

The most significant development during this reporting period is that the EU-U.S. Data Privacy Framework received an adequacy determination from the EU Commission and came into force on July 10, 2023. Privacy Shield participants

were seamlessly transitioned over to the EU-U.S. Data Privacy Framework. The UK Extension to the EU-U.S, Data Privacy Framework cannot be relied upon for UK to U.S. data transfers until the adequacy regulations implementing the data bridge come into force. Similarly, the Swiss-U.S. Data Privacy Framework cannot be relied upon for Switzerland to U.S. data transfers until the date of entry into force of its recognition of adequacy, However organizations may self-certify on the U.S. Department of Commerce's website and participate in the Framework for the EEA, UK, and Switzerland.

In light of this transition to the Data Privacy Framework, the Privacy Shield Compliance Verification service is now the TRUSTe Data Privacy Framework Verification. The name of the independent dispute resolution mechanism is unchanged and continues to be known as TRUSTe Dispute Resolution. All references to Privacy Shield have been changed to Data Privacy Framework throughout the remainder of this report.

TrustArc Inc, offers complimentary education and resources to participants in its Data Privacy Framework services including:

One-stop access to the Data Privacy Framework Update FAQs, webinars, and podcasts.

Seamless transition of the Privacy Shield Services to the Data Privacy Framework to support participants' continued compliance with the Framework principles

Technology resources to evaluate and assess data flows, identify data transfer risk and data transfer mechanisms, and address implementation gaps.

Provision of an alternative International Privacy Verification Program for verification of ongoing compliance with the Data Privacy Framework principles for participants that elect to withdraw from participation in the EU-U.S. Data Privacy Framework

A participant webinar series and consultations on the Data Privacy Framework to provide assistance with understanding the Framework and the transition to it from Privacy Shield.

REPORT OVERVIEW

This report includes information about:

- **The Data Privacy Framework services that TrustArc operates, including how we avoid conflicts of interest**
- **Participation in TRUSTe Data Privacy Framework Verification**
- **Participation in TRUSTe Dispute Resolution**
- **How complaints can be filed**
- **Data Privacy Framework complaint eligibility**
- **Complaint handling process**
- **Data Privacy Framework complaint statistics**

TrustArc DATA PRIVACY FRAMEWORK SERVICES

Data Privacy Framework Roles Served By TrustArc

TrustArc, under the TRUSTe brand, provides various external privacy compliance review programs for organizations seeking an independent review of whether they have met a particular privacy standard or set of privacy requirements. One of the programs we provide to organizations is an outside review of Data Privacy Framework compliance in accordance with Data Privacy Framework Supplemental Principle 7(d), which we call "TRUSTe Data Privacy Framework Verification." More details on this service are provided below.

A separate team at TrustArc, which operates independently from the team conducting outside compliance reviews, provides dispute resolution services, including dispute resolution services in fulfillment of a Data Privacy Framework Participant's independent recourse mechanism (IRM) obligations. Participants may utilize the IRM service without participating in the TRUSTe Data Privacy Framework Verification program.

TrustArc adheres to a Corporate Policy on Conflict of Interests, which requires segregation of duties between the team responsible for outside compliance reviews and the team responsible for dispute resolution services. The Privacy Assurance team conducting the outside compliance reviews reports to the Chief Assurance Officer, and the Compliance Team that provides dispute resolution services reports to the Chief Financial Officer. The routine processes and systems used by these teams do not overlap. Oversight of the program is led by the Legal Department with support from the Privacy Intelligence Team. Governance of the programs is coordinated among the aforementioned executive team members and the CEO.

In addition to these services, TrustArc offers individual consultations through our Data Privacy Framework Assessment Service, whereby a member of the Assurance Team assists a prospective Data Privacy Framework Participant in its evaluation of its privacy policies and practices against the Data Privacy Framework Principles. A findings report and action plan is then delivered, which includes a gap analysis and remediation recommendations.[1]

TrustArc also provides publicly-available FAQs in accordance with Data Privacy Framework Supplemental Principle 11(d)(ii)2[2] as well as a series of Data Privacy Framework webinars and blog postings[3].

During the Reporting Period		End of the Reporting Period	
Dispute Resolution Participants:	**Data Privacy Framework Verification Participants:**	**Dispute Resolution Participants:**	**Data Privacy Framework Verification Participants:**
342	219	316	172

[1] This analysis does not constitute an outside compliance review as the prospective Participants using this assessment-only service have opted to instead use the self-assessment verification methodology, utilizing the remediation recommendations received via the service guidance for their own determination of compliance.

[2] https://trustarc.com/consumer-info/dispute-resolution/dispute-resolution-faqs/

[3] https://trustarc.com/resource_types/webinars/ and https://trustarc.com/blog/2023/08/03/selecting-the-best-eu-us-data-transfer-mechanism/ and https://trustarc.com/blog/2023/07/19/business-eu-us-data-privacy-framework-verification/

PARTICIPATION IN TRUSTe DATA PRIVACY FRAMEWORK VERIFICATION

TrustArc offers outside compliance reviews in accordance with Supplemental Principle 7 - Verification. In order to participate in the TRUSTe Data Privacy Framework Verification program, a Participant must be a U.S. legal entity subject to the jurisdiction of either the Federal Trade Commission or the Department of Transportation, agree to be assessed for compliance with the Data Privacy Framework Principles in accordance with the TRUSTe Data Privacy Framework Verification Program Assessment Criteria,[4] and agree to comply with the TRUSTe Assurance Program Governance Standards.[5]

Verification Process

The Verification Process involves three steps:

Assessment: TrustArc performs an initial assessment of compliance;

Remediation and Verification: TrustArc provides a report and action plan to program applicants outlining our findings regarding compliance with the Data Privacy Framework Principles. TrustArc then verifies that the required changes provided in the report and action plan have been properly implemented; and

Monitor: TrustArc verifies ongoing compliance with the Assessment Criteria and Assurance Program Governance Standards.

Upon successful completion of the assessment and verification process, and completion of Data Privacy Framework self-certification with the U.S. Department of Commerce indicating TRUSTe as its outside compliance reviewer, Participants in the TRUSTe Data Privacy Framework Verification program are issued the TRUSTe Verified Privacy seal along with authorization to display it.

Compliance Monitoring

After a Participant completes its self-certification and appears on the Active Data Privacy Framework List, TrustArc uses a combination of approaches to monitor compliance with the requirements for participation in the TRUSTe Data Privacy Framework Verification program, including continued adherence to the Data Privacy Framework Verification Program Assessment Criteria and the TRUSTe Assurance Program Governance Standards.

[4] Available online at https://trustarc.com/pdf20/DPF-Assessment-Criteria-07072023.pdf
[5] Available online at https://download.trustarc.com/?f=4OB4NEWY-742

These methods include:

Implementation Checks: Within six (6) months of the Participant's initial certification or certification renewal, TrustArce's Quality Improvement Team (QI Team) will conduct a check to verify the privacy notice approved by TrustArc is the one that is available on the participant's online properties. The QI Team also verifies that the seal is implemented properly, and displayed on approved privacy notices.

TRUSTe Feedback and Resolution System: Defined in detail in the section below on TRUSTe Dispute Resolution, TrustArc investigations may be initiated after a media report, regulator inquiry, or information obtained through other credible sources.

Compliance Investigations

Beyond compliance monitoring, TrustArc also has a review process to investigate a suspected breach of the Data Privacy Framework Verification Program Assessment Criteria, and the TRUSTe Assurance Program Governance Standards. This process is led by the Compliance team, which reports to the Chief Financial Officer, and is typically conducted under the direction of the Legal Department. It begins with an internal compliance investigation. TrustArc may initiate this investigation based on results of our monitoring, based on information contained in a consumer complaint, media reports, regulator inquiries, or reports from other credible sources. Where non-compliance with the requirements set forth in the Data Privacy Framework Verification Program Assessment Criteria and the TRUSTe Assurance Program Governance Standards is found, TrustArc will investigate the compliance issue, notify the Participant, outline the necessary corrections, and provide a reasonable timeframe for the Participant to make such changes, during which time TrustArc works with the Participant to ensure the necessary changes are made. TrustArc compliance investigations may result in one of the following three outcomes:

Agreement and Resolution: An agreement between TrustArc and the Participant over the privacy complaint resulting in resolution by the Participant that addresses the concern or request. TrustArc provides a reasonable timeframe to complete the required changes based on the risk and level of non-compliance;

Formal Enforcement: A disagreement triggering a notice of formal enforcement, resulting in the Participant's suspension or notice of intent to terminate for cause if the matter is not cured or

Termination: A failure to implement the required cure resulting in TrustArc terminating the Participant from the program, and in extreme cases, publication and/or referral to the appropriate authority.

Participation

TrustArc provides a periodic list of Participants to the Department of Commerce. As of the close of this annual reporting period, the following number of Participants had been verified, either as a stand-alone service for HR Data (27 Participants), or for Non-HR Data, in combination with TRUSTe Dispute Resolution services.

TRUSTe Data Privacy Framework Verification Participants:
172

PARTICIPATION IN TRUSTe DISPUTE RESOLUTION

TrustArc offers dispute resolution services in fulfillment of a participant's Independent Recourse Mechanism obligations set forth in Principle 7 - Recourse, Enforcement, and Liability and Supplemental Principle 11 - Dispute Resolution and Enforcement. In order to participate in the TRUSTe Data Privacy Framework Dispute Resolution program, a Participant must be a U.S. legal entity subject to the jurisdiction of either the Federal Trade Commission or the Department of Transportation and agree to the TRUSTe Dispute Resolution Procedures, which in summary include:

- At the time of agreement, or as soon as practicable thereafter, provide a copy of the privacy notice(s) applicable to its participation in the Data Privacy Frameworks;
- Provide individuals with simple means to submit complaints and express their concerns regarding the Participant's privacy practices and respond timely to submissions;
- Cooperate with TrustArc to resolve complaints, disputes, questions, and concerns in accordance with the detailed process described in the TRUSTe Privacy Dispute Resolution FAQs;[6]
- Abide by the dispute eligibility determinations of TrustArc;
- Timely acknowledge and respond to applicable inquiries from TrustArc; and
- Submit to reviews to resolve disputes regarding its compliance with the applicable requirements as described under the Compliance Investigations section above.

[6] https://trustarc.com/dispute-resolution-faqs/

HOW COMPLAINTS CAN BE FILED

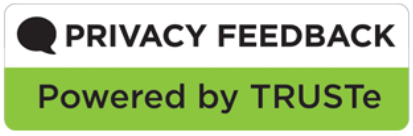
TrustArc provides privacy resources for consumers related to the Data Privacy Framework online,[7] including access to the following:

- **An online form to file a complaint**
- **Dispute Resolution FAQs**
- **Data Privacy Framework Supplemental Principle 11(d) on Recourse Mechanisms**
- **Access to dataprivacyframework.gov/s/**
- **Access to its Annual Data Privacy Framework Reports**

Filing a complaint requires just two simple steps:

Step 1

A Data Privacy Framework-related complaint can be filed by a consumer by either clicking the "Privacy Feedback" button or directly through https://feedback-form.truste.com/watchdog/request, based on which mechanism is made available by the Participant in its privacy notice. All TRUSTe Data Privacy Framework Dispute Resolution Participants are required to display either the foregoing link or the Privacy Feedback button to the right as a condition of participation.



Step 2

The complainant must then provide the following information as requested in the feedback form:

- ✓ **The name of the Participant the complainant wishes to report (including the site URL)**
- ✓ **The complaint type as provided in a drop down menu**

[7] https://trustarc.com/data-privacy-framework/

- ✓ **A narrative description of the issue**
- ✓ **The date when the complainant attempted to contact the Participant regarding the listed concern[8]**
- ✓ **The Participant's response**
- ✓ **The resolution sought by the complainant**
- ✓ **The complainant's email address[9]**
- ✓ **The complainant's name[10]**
- ✓ **The complainant's country**
- ✓ **Permission for TrustArc to share the information provided by the complainant with the Participant in question in order to resolve the issue[11]**

[8] Before submitting a complaint to TRUSTe, a complainant should attempt to contact the Participant directly to allow them reasonable time to resolve the concern.
[9] If the complainant wishes to receive a response or be reachable for questions and updates, they must provide a working email address where they can receive email. Certain requests, such as those related to a specific action affecting the complainant may be unable to be resolved without being able to provide identifying information to the Participant about whom the complaint is made.
[10] Complainants are welcome to use their real name or use a "No Name" option if they prefer.
[11] Refusal to provide permission may limit the ability of the named Participant to address the stated concern.

DATA PRIVACY FRAMEWORK COMPLAINT ELIGIBILITY

General Eligibility

In order for a complaint to be considered eligible for resolution by TrustArc, all of the following 6 conditions must be met:

- ✓ The complaint is about an organization that either is a Participant in a TRUSTe Assurance Program who holds an authentic TRUSTe seal or is a Participant in a TRUSTe Dispute Resolution program;
- ✓ The complainant has already made a good faith attempt to resolve the problem directly with the Participant, allowing them reasonable time to respond;
- ✓ The complaint raises a privacy issue that affects the Personal Information[12] of either the complainant or of a child for whom the complainant is the parent or guardian;
- ✓ The complaint alleges that the Participant collected, used, or disclosed the Personal Information in a manner inconsistent with its published privacy notice;
- ✓ The complaint is in English or the Participant has secured appropriate translation services; and
- ✓ The complaint is submitted to TrustArc via the online TRUSTe Dispute Resolution form.[13]

Determination of Data Privacy Framework-Related Complaints

For purposes of the statistics provided in this report, a complaint must further meet the following criteria to be considered an eligible Data Privacy Framework-related complaint:

- ✓ The complainant is an EEA, Gibraltar, UK or Swiss individual (i.e., the individual submitting on his or her own behalf or on behalf of a minor of whom the individual is a parent or guardian);
- ✓ The complaint concerns a Participant in the TRUSTe Data Privacy Framework Dispute Resolution program;
- ✓ The complaint concerns an organization participating in a Department of Commerce-administered Data Privacy Framework program; and
- ✓ The complaint alleges that an organization has violated the Data Privacy Framework Principles with respect to the complainant's own Personal Information or the Personal Information of a minor of whom the complainant is the parent or guardian.

COMPLAINT OVERVIEW

51	1
Complaints Received from Individuals in the EEA, Gibraltar, UK, and Switzerland	**Data Privacy Framework-Related Complaints Addressed**

[12] Data about an identified or identifiable individual
[13] https://feedback-form.truste.com/watchdog/request

COMPLAINT HANDLING PROCESS

Following receipt of a Dispute Resolution request, TrustArc will inform the filing complainant within ten (10) business days as to whether the complaint meets the eligibility requirements or whether TrustArc needs further information to make such a determination. If further information is needed, a complainant has fourteen (14) calendar days from the date of TrustArc's request to provide this additional information. If it is determined that the complaint is ineligible, the complainant will be emailed a written notification. If the complaint is deemed eligible, TrustArc will request a response from the Participant within fourteen (14) calendar days.

Once TrustArc has made a final determination about the complaint, it will inform the complainant and, if applicable, the Participant. At that time, either party may file an appeal within fourteen (14) calendar days. Upon receiving an appeal, TrusArc's Compliance Director will review the appeal and determine within ten (10) business days whether the complaint is eligible to be reopened for further investigation. After TrustArc's Compliance Director completes review of the appeal request, TrustArc may direct the other party to respond by email within ten (10) business days thereafter, explaining why TrustArc's final determination should be sustained, or supplying responses to specific questions from TrustArc. If TrustArc's Compliance Director determines that the original complaint disposition was proper according to TrustArc's processes, and introduces no substantive new information that could not have been raised earlier, or finds no other basis for appeal, the Compliance Director will request review by the Legal Department of the issue appealed, and TrustArc will respond with its final appeals determination within ten (10) business days. If a Participant fails to answer a question with a timely response, TrustArc will send a second notice to the Participant and attempt phone notification. If the issue remains unresolved, TrustArc will withdraw or suspend the Participant's use of TRUSTe Dispute Resolution Services, notify the Department of Commerce of the organization's failure to comply, and/or take other action as necessary, including referral to the appropriate enforcement authority depending on the nature of the complaint.

Participation

As of the close of this annual reporting period, 316 Participants were enrolled in the TRUSTe Data Privacy Framework Dispute Resolution service. This included 144 participants in TRUSTe Dispute Resolution only and 172 participants in TRUSTe Compliance with Dispute Resolution for Non-HR Data.

Data Privacy Framework Dispute Resolution Participants:
316

DATA PRIVACY FRAMEWORK COMPLAINT STATISTICS

From August 1, 2022 through July 31, 2023, TrustArc handled 51 complaints from individuals located in the EEA, Gibraltar, UK, and Switzerland. The below details the types of complaints TrustArc received about Data Privacy Framework Dispute Resolution participants by the Data Privacy Framework Principle to which the complaint type aligns, country where the complainant is located, and by type of complaint.

Data Privacy Framework Principle		Complainant Location		By Type	
Choice	2	Belgium (BE)	2	Account Hacked / Disabled / Suspended	7
Data Integrity and Purpose Limitation	8	Bulgaria (BG)	1	Can't Change / Remove Personal Info	11
Access	11	Croatia (HR)	1	Help with Features / Functionality	4
Recourse, Enforcement, and Liability	17	Cyprus (CY)	1	Monetary / Billing / Transactional	2
Other	13	Denmark (DK)	1	Received Unauthorized E-Mail	1
		Finland (FI)	2	Shared Personal Info with Unauthorized Third Party	1
		France (FR)	9	Unable to Contact Participating Site	17
		Germany (DE)	7	Unable to Unsubscribe	1
		Hungary (HU)	2	Undefined e.g. Random Typing/Incomprehensible	7
		Italy (IT)	1		
		Netherlands (NL)	3		
		Poland (PL)	9		
		Portugal (PT)	3		
		Spain (ES)	4		
		Sweden (SE)	3		
		Slovakia (SK)	2		
Totals	**51**		**51**		**51**

Data Privacy Framework-Related Complaints

Of the 51 complaints received from individuals in the EEA, Gibraltar, the UK, or Switzerland, one (1) involved requests eligible for resolution. Ineligible complaints include issues where:

- **Subject matter:** The subject matter of the request was not eligible, such as billing requests not alleging an eligible issue, where the individual seeks to access information or make data changes about another individual for whom the complainant is not the parent or guardian, or the issue was incomprehensible, such as random typing.
- **Procedural grounds:** The complaint was closed on procedural grounds such as duplicates, where the individual withheld consent for TRUSTe to share his or her identity to allow the Participant to research the issue, where the complainant failed to contact the Participant, where the complaint was misfiled against a Participant when the complaint related to another company, or where the complainant dropped the request.

The next table shows how the resolution of those complaints were classified and resolved by TrustArc. No complaints were pending resolution at the close of the reporting period.

Complaint Resolution Classification	Number of Complaints Resolved
Procedural grounds *Procedural grounds may include:* • *Complaints that fail to state a comprehensible issue or even a complete word (e.g. random typing such as "xyxyxy");* • *When the complaint did not give TRUSTe permission to pass identifying information to the company in question; or* • *The complainant provided an invalid e–mail address, impeding investigation of that complaint.* • *Duplicate compliant* • *No response from the consumer*	**19**
Out of scope *Out of scope are complaints that fall into categories that are outside the scope of TRUSTe's authority under its Assurance Programs, (e.g., billing/transactional issues, requests for feature enhancements). TRUSTe typically suggests that the complainant contact the company directly in these instances.*	**14**
Consumer education by TRUSTe	**15**
Personal information removed, account closed, or credentials validated	**1**
Action taken without involvement from TRUSTe	**1**
TRUSTe's assistance in facilitating resolution was required, but no changes were required from the participating company.	**1**
Total	**51**

Dispute Resolution Quality Measures

As described in the section above on the Complaint Handling Process, once a complaint has been reviewed and referred to the Participant for response, the Participant ordinarily has ten (10) business days to provide a written response for the complainant. For more urgent issues, such as security vulnerabilities, we escalate to the Participant via phone as well and generally expect responses much sooner, especially if we are able to verify the problem. If a Participant fails to answer a complaint with a timely response, TrustArc will send a second notice to the Participant and attempt additional outreach, including phone notification. If the issue remains unresolved, TrustArc will:

- Withdraw or suspend the Participant's use of Dispute Resolution services;
- Notify the Department of Commerce of the organization's failure to comply; and/or
- Take other action as necessary, including referral to the appropriate enforcement authority depending on the nature of the complaint.

No complaints received during the reporting period required escalation due to a Participant's failure to resolve. The average resolution time for Privacy Shield complaints (including those determined to be ineligible) received during the reporting period was six (6) calendar days. The table below shows the resolution time for the complaints received by the TRUSTe Data Privacy Framework Dispute Resolution service.

Number of Complaints	Time to Resolution
25	Less than 24 hours
12	1-9 calendar days
13	10-19 calendar days
1	Greater than 20 calendar days

For complaints eligible for resolution (excluding those closed on procedural grounds as described above), TrustArc notifies the complainant and, if applicable, the Participant of the resolution. In all instances, TrustArc asked the complainant to provide consent before sharing Personal Information about them with the Participant in question. All Personal Information collected during the Dispute Resolution process is handled in accordance with the TrustArc Privacy Policy (available at https://trustarc.com/privacy-policy/).

ABOUT TrustArc

TrustArc automates the creation of end-to-end privacy management programs for global organizations. As the leader in privacy compliance and data protection, TrustArc is the only company to deliver the depth of privacy intelligence that's essential for the growing number of privacy regulations in an ever-changing digital world. TrustArc powers privacy compliance and risk management with integrated technology, consulting and TRUSTe Assurance Program solutions – addressing all phases of privacy program management.

Headquartered in California, and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk and build trust. For additional information visit www.trustarc.com.

TRUSTe Assurance Programs, such as our Data Privacy Framework Compliance Verification Program and our TRUSTe Dispute Resolution services, are provided by TruatArc Inc under its TRUSTe brand.

Questions regarding this report should be directed to the Legal Department at legal@trustarc.com

TrustArc