EU Privacy Shield

BBB PROCEDURE REPORT

Compliance activities and casework conducted by CBBB's BBB EU Privacy Shield Program from August 1, 2017 through July 31, 2018

Frances J. Henderson, J.D., CIPP/U.S.,
Vice President and National Director, Privacy Initiatives

Bryant C. Fry, FIP
Deputy Director, BBB EU Privacy Shield

Council of Better Business Bureaus

EXECUTIVE SUMMARY

The period covered by this report, August 1, 2017 through July 31, 2018, constituted the second year of BBB EU Privacy Shield (BBB EUPS) operations. The program was created by the Council of Better Business Bureaus in 2016 as an Independent Recourse Mechanism supporting the Privacy Shield Frameworks. It provides both independent dispute resolution and compliance assistance to participating companies.

The second year of program operations was marked by:

- Assisting companies in navigating the payments process for the Arbitral Fund launched in September 2017, which is meant to cover the costs of handling residual arbitration claims under Annex 1.
- Participating as one of two Independent Recourse Mechanisms invited to address the First Annual Review of Privacy Shield in September, 2017.
- Advising program participants about the reports issued by the European Commission and Article 29 Working Party in October 2017 following the Annual Review.
- Assisting participants and new applicants in matching their privacy policies with the requirements of Privacy Shield and providing educational resources to help companies seeking to align their practices with the EU General Data Protection Regulation (GPDR).

YEAR IN REVIEW

Participation. BBB EUPS increased enrollment during the review period from around 700 companies in July 2017 to around 1,000 participants as of July 31, 2018.

Outreach. BBB EUPS has continued to publish periodic participant newsletters and online Privacy Shield compliance guidance for program applicants and the business community. Responding to business demand, in early 2018 the program launched dedicated online resource pages for companies seeking to align their privacy practices with GDPR and also established a privacy blog covering Privacy Shield and GDPR topics. In May 2018, BBB co-presented a webinar[1] with the U.S. Department of Commerce, providing tips for complying with the GDPR and Privacy Shield.

Compliance Activities. BBB EUPS continues to provide all program applicants with privacy policy guidance, and assists them as needed with self-certification and recertification. The program also monitors participants' online privacy policies and Privacy Shield self-certifications on an ongoing basis for changes that may affect compliance, and provides automatic reminders to companies before their self-certifications are due for renewal.

Complaint Handling. The program received 525 complaint submissions, including 101 from the EU and Switzerland, through the BBB EUPS online complaint form. Following a review of each complaint by program staff, all but two complaints were determined to be ineligible for resolution by the program for one or more of the following reasons: they concerned companies not enrolled in BBB EUPS; they did not involve data collected in the EU or Switzerland; they were unrelated to privacy (i.e., product or service complaints); or they failed to state a complaint. The remaining two complaints were incomplete as submitted, and were dropped by complainants before sufficient information could be obtained to establish eligibility.

[1] Available at: https://bbbprograms.org/programs/bbb-privacy-shield/gdpr-webinar-Q-A/.

ABOUT THE PRIVACY SHIELD FRAMEWORKS

The General Data Protection Regulation (GDPR)—like its predecessor, the Data Protection Directive—prohibits transfers of personal data from the European Union to destinations, including the United States, that do not meet the European "adequacy" standard for privacy protection. U.S. companies therefore must use an "adequate" data transfer mechanism to receive and process personal data from Europe.

On July 12, 2016, the U.S. Department of Commerce and the European Commission announced the launch of the EU-U.S. Privacy Shield Framework for transatlantic data flows to replace the U.S.-EU Safe Harbor, which was invalidated by a decision of the European Court of Justice in October 2015. While retaining many elements of Safe Harbor, Privacy Shield includes enhanced consumer privacy protections for EU individuals, promotes greater transparency around data collection, use, and sharing, and helps U.S. companies demonstrate that their privacy practices meet EU data protection requirements.[2]

On January 12, 2017, the Swiss Government approved the Swiss-U.S. Privacy Shield Framework as a valid legal mechanism for U.S. companies to comply with Swiss data protection requirements when transferring personal data from Switzerland to the United States. The U.S. Department of Commerce began accepting self-certifications for this Framework on April 12, 2017.

Companies participating in either Privacy Shield Framework must submit a self-certification application to the Department of Commerce, stating their adherence to the Privacy Shield Principles for personal data they receive from the EU or Switzerland. Participating companies are required to maintain a current self-certification on the official EU-U.S. or Swiss-U.S. Privacy Shield Lists maintained by the Department of Commerce. As of September 13, 2017, each participating company must contribute to the Arbitral Fund, which is intended to support the operation of the Annex 1 arbitration mechanism for residual complaints that remain unresolved by multiple redress mechanisms, including referrals to the EU Data Protection Authorities and the Swiss Federal Information Commissioner.

Participants must also verify on an annual basis that their public attestations regarding their Privacy Shield privacy practices are accurate, through self-assessment or outside compliance reviews; and must provide an independent dispute resolution option—also called an Independent Recourse Mechanism or IRM—to handle privacy complaints from EU and Swiss individuals whose personal data they process.

ABOUT BBB EU PRIVACY SHIELD

On July 12, 2016, immediately following the formal adoption of the Privacy Shield Framework for EU-U.S. data transfers, the Council of Better Business Bureaus (CBBB) launched BBB EU Privacy Shield (BBB EUPS) as an Independent Recourse Mechanism to support the new Framework.

In its second year of operation, BBB EUPS provided services to around one thousand companies, more than 860 of which were self-certified as of July 31, 2018. The program, which has expanded steadily since its inception, experienced strong growth in the first half of 2018, as many U.S. companies began actively aligning their privacy practices with the requirements of the GDPR, which came into effect May 25, 2018.

This annual report summarizes the ongoing compliance activities and casework of CBBB's BBB EUPS program spanning August 1, 2017 through July 31, 2018.

[2] The Commission Decision on the adequacy of the protection provided by the EU-U.S. Privacy Shield applies to the 28 EU member states, and also to Iceland, Liechtenstein, and Norway. Thus, references in this report to the European Union (EU) should be read as including Iceland, Liechtenstein, and Norway.

→ IN ITS SECOND YEAR OF OPERATION, BBB EUPS PROVIDED SERVICES TO AROUND ONE THOUSAND COMPANIES, MORE THAN 860 OF WHICH WERE SELF-CERTIFIED AS OF JULY 31, 2018.

BBB EU PRIVACY SHIELD CORE REQUIREMENTS

Each applicant to join BBB EU Privacy Shield provides the program with a copy of the consumer-facing Privacy Shield privacy notice to be posted on its public website. BBB EUPS staff reviews the privacy policy for basic compliance with Notice Principle requirements, and notably, for the inclusion of a live hyperlink to the BBB EU Privacy Shield consumer information web page and online complaint form.

Participation Agreement

Each BBB EU Privacy Shield participant must agree:

- To upload the privacy policy approved by BBB EUPS to the Department of Commerce website during the self-certification process and, following Commerce Department approval, to post and maintain the privacy policy on all company websites to be covered by Privacy Shield;
- To notify BBB EUPS of all changes to the posted policy, including any changes required by the Department of Commerce during the self-certification process, and to provide BBB EUPS a copy of the updated policy;
- To apply for self-certification with the Department of Commerce within 30 days of acceptance into the BBB EUPS program, and to maintain a current self-certification for the duration of its participation in BBB EUPS;
- To cooperate with BBB EUPS staff to respond to privacy complaints in accordance with the BBB Procedure Rules;
- In cases sent to a Data Privacy Review before an independent Data Privacy Panelist, to accept the Panelist's final decision; and
- To implement any corrective action agreed to as part of a settlement, or mandated by a Panelist's decision.

These requirements are incorporated in a Participation Agreement that is renewable annually following a BBB EUPS staff review of the company's online Privacy Shield privacy policy and self-certification listing to ensure that the company remains in compliance.

Review of Privacy Policies/Practices

BBB EU Privacy Shield staff examines applicants' online privacy policies and any referenced terms and conditions for clarity, completeness, and for the inclusion of all elements required by the Privacy Shield Notice Principle. Applicant companies can access detailed resources about the Privacy Shield Principles and the self-certification process on the program website (bbb.org/EU-privacy-shield/privacy-policy-requirements). We provide additional privacy policy guidance and tips during the application process, including the following:

- Ensure the privacy policy is clearly written and is readily accessible on the company's public website.
- Ensure that the applicant company clearly identifies the corporate entity or entities processing EU or Swiss personal data pursuant to Privacy Shield. If a brand name or d/b/a is used on the company's public website(s), the company's legal name should also appear in the policy, in its self-certification, and also in the BBB EU Privacy Shield Participation Agreement. This information can facilitate a consumer's search for the appropriate company on the official Commerce Department Privacy Shield List and in the BBB EU Privacy Shield complaints system.
- Where multiple entities and web domains are to be covered by a master corporate privacy policy, ensure that each covered website includes the correct policy and the active hyperlink to the BBB EU Privacy Shield consumer pages and complaint system.

COMPLIANCE ACTIVITIES AND KEY ISSUES 2017-18

Companies enrolling in BBB EU Privacy Shield during the second year of program operations ranged from large multinational corporations to small and mid-sized businesses across multiple industry sectors. Applicants seeking self-certification assistance from BBB EU Privacy Shield were closely engaged in adapting their public and internal privacy policies and practices to meet new transparency and compliance obligations, and in many cases, were seeking to align their policies and practices with GDPR requirements.

First Annual Review and Changes in Self-Certification Process

After the first Annual Review discussions held in Washington, DC in September 2017, both the European Commission and the Article 29 Working Party produced reports reflecting on the first year of the Privacy Shield Frameworks. In the wake of these discussions, the U.S. Department of Commerce implemented some changes to its Privacy Shield certification process and released updated step-by-step guidance on this process. Most notably, this included a requirement for companies to receive pre-authorization for their Privacy Shield-related privacy policy statements before posting policies that publicly claim self-certification. The Department of Commerce also clarified its guidance on the listing of company subsidiaries, and committed to ongoing randomized reviews of Privacy Shield participants.

BBB EUPS staff educated our existing participants on these changes and adjusted our program guidance accordingly. We also distributed guidance about changes to the certification process to the business community on our program website and to our participants and applicants in newsletters, service messages, and one-on-one consultations. We continue to work closely with new applicants to ensure that they follow all current requirements of the certification process. This helps ensure that our list of program participants remains accurate and complete, while also facilitating timely completion of the process for each participant.

GDPR Compliance

The implementation of GDPR sparked renewed interest among U.S. businesses in self-certifying to Privacy Shield, and prompted BBB EUPS to offer additional guidance and resources to program participants.

Though BBB EUPS does not provide individualized GDPR services, we have made a strong push this year to provide our applicants and participants with accurate information about the changes in EU privacy law brought about by GDPR. We have posted guidance on our informational web pages (https://bbbprograms.org/programs/bbb-privacy-shield/GDPR-resources) along with links to outside resources, and we continue to discuss GDPR topics in ongoing blog posts and in our periodical newsletter for participants.

Many Privacy Shield participants now include language in their privacy policies addressing GDPR compliance in addition to required language about their compliance with Privacy Shield as a valid transfer mechanism under GDPR. As an IRM, our primary goal is to ensure that participant privacy policies incorporate all required Privacy Shield elements without creating confusion for the reader. Where a policy also addresses GDPR compliance, we seek to ensure that the policy fully articulates the rights and obligations applicable to data transfers under Privacy Shield independently from the general GDPR requirements, with all rights and remedies clearly enumerated. Most importantly, we ensure that the policy directs privacy inquiries and complaints under GDPR and Privacy Shield to the appropriate redress mechanisms. Many Privacy Shield participants now include language in their privacy policies about general GDPR compliance in addition to required language about their compliance with Privacy Shield as a valid transfer mechanism under GDPR. As an IRM, our primary goal is to ensure that participant privacy policies address all required Privacy Shield requirements without causing confusion for the reader. Where a policy also addresses GDPR compliance, we seek to ensure that the policy fully articulates the rights and obligations applicable to data transfers under Privacy Shield independently from the general GDPR requirements, with all rights and remedies clearly enumerated. Most importantly, we ensure that the policy directs privacy inquiries and complaints under GDPR and Privacy Shield to the appropriate redress mechanisms.

→ THE IMPLEMENTATION OF GDPR SPARKED RENEWED INTEREST AMONG U.S. BUSINESSES IN SELF-CERTIFYING TO PRIVACY SHIELD, AND PROMPTED BBB EUPS TO OFFER ADDITIONAL GUIDANCE AND RESOURCES TO PROGRAM PARTICIPANTS.

DISPUTE RESOLUTION AND ENFORCEMENT

BBB EU Privacy Shield's self-regulatory dispute resolution procedures are designed with two primary goals in mind. First, to ensure that the privacy concerns of individual complainants concerning data collected in the EU or Switzerland are addressed speedily and impartially. Second, to promote privacy accountability among U.S. companies participating in the program.

BBB EU Privacy Shield provides a secure, accessible online mechanism for handling privacy complaints under the Privacy Shield Principles by individuals against participating U.S. businesses.

The service is provided free of charge to individuals, who can readily access the BBB EUPS online complaint form through a live hyperlink each participating company must include in the privacy policy posted on its public website.

The dedicated link first takes the site visitor to BBB EU Privacy Shield's consumer-facing web page entitled "For EU and Swiss Consumers" which describes the program's role as an IRM and how our complaint process works.[3] From this page, the site visitor clicks a prominent "File a Complaint" button to gain direct access the BBB EUPS complaint form. On a second page linked from the main consumer-facing page, entitled "How to File a Complaint with BBB EU Privacy Shield," visitors can also find a mailing address to communicate with the program by postal mail.

The BBB EUPS complaint form can also be accessed through the BBB Online Complaint System. The main "File a Complaint" link found on the home page of the BBB national website, as well as on pages throughout the site, enables privacy complainants to navigate through a series of screens to the dedicated BBB EUPS page.

Complaint Handling Rules and Procedures

Eligibility

As provided in the program's Procedure Rules,[4] BBB EUPS staff first reviews each incoming complaint to determine its eligibility for resolution under the program. The first step is to confirm that the company complained about is a current program participant and therefore within the program's scope. For participating companies, next steps in the process may include seeking additional information from the complainant, such as the complainant's location or country of residence, the location of the data collection, or additional identifying information, and clarifying the exact nature of the complaint. Language translation services are available for use as needed to facilitate any or all stages of the complaint handling process.

Conciliation

When a complaint is found eligible, BBB EUPS staff will open a case and will work with the complainant and the participating business to facilitate a resolution of the complaint. In the BBB EU Safe Harbor program, it was our experience that most complainants followed this conciliation approach to reach a satisfactory settlement of the issue with the participating company.

Data Privacy Review

If conciliation efforts are unsuccessful, either the complainant or the participating company may request a Data Privacy Review, which will take the form of a hearing and decision based on the Case Record, including the positions of each of the parties regarding the complaint, submitted by BBB EUPS staff to an independent panelist on the program's

[3] See https://www.bbb.org/EU-privacy-shield/for-eu-consumers. While the program welcomes complaints from individuals in the U.S. or in other countries who claim that their data was collected in the EU or Switzerland and transferred to the United States pursuant to Privacy Shield, we pay particular attention to ensuring access by EU and Swiss data subjects.

[4] Available at: https://www.bbb.org/EU-privacy-shield/rules-and-policies/.

Data Privacy Board. The panelist has discretion to seek additional written information from the parties or to convene a telephone hearing if necessary, before issuing a final decision.[5]

Participating companies that fail to comply with BBB EUPS Data Privacy Review procedures, including failing to take agreed upon action following conciliation, or failing to implement mandated corrective action following the final decision of the independent Data Privacy Board panelist, may be referred to the appropriate federal government agency—generally the Federal Trade Commission—and the referral will be reported to the Department of Commerce. In such a case, the program is required to publish in the Annual Procedure Report the name of the participating company and the fact of the referral, along with a summary report of the facts of the case and the Procedure's action in the matter.[6]

Compliance Verification and Additional Redress Options

BBB EU Privacy Shield verifies the company's compliance with both conciliated settlements and mandated corrective action. This includes seeking confirmation from the complainant that the matter has been resolved to his or her satisfaction. The case is then closed. However, the complainant is not bound by the outcome of the BBB EUPS dispute resolution procedure, and may pursue all additional redress options available under Privacy Shield, up to and including the binding arbitration procedures provided for in Annex 1.

2017-18 BBB EU PRIVACY SHIELD CASEWORK

Each year, the BBB Online Complaints System handles more than 800,000 general consumer complaints against U.S. and Canadian businesses from consumers in North America and worldwide. These include product and service complaints, as well as some privacy-related matters. The overwhelming majority of BBB complaints are submitted by North American consumers. About 1,200 general consumer complaints handled by the BBB system during the period of review for this report originated in the EU or Switzerland.

BBB EU Privacy Shield complaint data provided in this report does not include these general consumer complaints. The report addresses only complaints submitted to the program through the dedicated Privacy Shield online complaint form located at https://www.auto.bbb.org/eu-privacy-shield-complaint-form/.

BBB EU Privacy Shield Complaints Analysis

During the review period, BBB EU Privacy Shield (BBB EUPS) received a total of 525 complaints, almost a threefold increase from the 2016-2017 period.

Complaint Profiles by Country of Origin

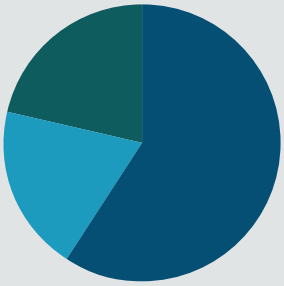
The breakdown of complaints received by country of origin demonstrates that the BBB EUPS dispute resolution service is readily accessed by complainants from a diverse group of countries, including the EU and Switzerland. Of 525 complaints reviewed, 313 were submitted by U.S. residents; 101 were submitted by individuals claiming residence in 21 EU countries plus Switzerland; and 111 were received from individuals residing in 30 other countries outside the EU.

[5] See Part 4 of the Procedure Rules: https://www.bbb.org/EU-privacy-shield/rules-and-policies/.

[6] See Section 8.8 of the Procedure Rules: https://www.bbb.org/EU-privacy-shield/rules-and-policies/.

The table below shows the breakdown of complaints received by region and country.

Complaints Received by Geographic Region



313 Complaints submitted by U.S. residents

101 Complaints received from individuals in the EU and Switzerland

111 Complaints received from individuals in other non-European countries

Breakdown of EU and Swiss Complaints Received by Country of Residence

Belgium	1	Lithuania	2
Bulgaria	1	Luxembourg	1
Czech Republic	1	Norway	2
Denmark	2	Netherlands	4
Estonia	1	Poland	4
France	1	Romania	2
Germany	10	Slovenia	1
Greece	2	Spain	7
Hungary	4	Sweden	1
Ireland	1	Switzerland	5
Italy	1	UK	47

Complaint Eligibility Analysis

BBB EUPS received a total of 525 complaint submissions during the 2017-2018 reporting period. Following an eligibility review of each complaint, which included requesting additional information from the complainant wherever appropriate, none of the complaints received was ultimately found eligible for disposition by the program.

The largest category of ineligible complaints concerned companies not participating in the BBB EUPS program. We received 502 such out-of-scope complaints, comprising around 95 percent of the total complaints received. Although ineligible for resolution under our program, BBB EUPS reviewed each complaint carefully. For complaints closed as ineligible, BBB EUPS sought to direct complainants to an alternative dispute resolution mechanism whenever appropriate.[7]

A total of 23 complaints were received against BBB EUPS participating companies. Of these, 21 were closed as ineligible for the following reasons:

- Six complaints did not originate from an EU or Swiss resident and did not otherwise allege data collection in the EU or Switzerland and transfer to the United States.
- Two complaints were unrelated to data collection (product or service complaints).
- Thirteen complaint submissions were closed as invalid because the content did not state a complaint (comments unrelated to privacy or unintelligible).

The two remaining complaints claimed U.S. processing of data collected in the EU or Switzerland. Both complaints were incomplete as submitted, and were closed after complainants failed to respond to BBB EUPS staff requests for additional information required to determine eligibility.

[7] Where an ineligible complaint concerned a U.S. business not self-certified on Privacy Shield, BBB EUPS staff directs the complainant to the Better Business Bureau Online Complaint System for alternative dispute resolution. For cases indicating a potential privacy complaint against a business self-certified on Privacy Shield with another IRM, staff directs the complainant to the company's self-certification listing indicating the correct IRM. For a privacy complaint concerning a business located in the EU or Switzerland, the complainant is directed to the national Data Protection Authority.

EU and Swiss Complaints Analysis

A total of 101 complaints originated in 21 EU countries and Switzerland. All but six complaints were directed against companies not currently participating in the BBB EUPS program. (Sixty of these 95 out-of-scope complaints did, however, express data privacy concerns about U.S. companies.) Of the six complaints concerning BBB EUPS participants, four were product or service complaints unrelated to privacy. The two remaining complaints were incomplete as filed. Each was dropped by the complainant following a request for additional information and before the eligibility review could be completed.

Observations

As has previously been our experience with Privacy Shield, the majority of complaints received were directed against companies that were either not enrolled in BBB EUPS or not self-certified to Privacy Shield at all. The number of complaints received from the EU or Switzerland during this reporting period almost doubled over the previous period of review, and a majority of those complaints concerned privacy. These statistics suggest that EU and Swiss data subjects can readily access, and are prepared to engage with the BBB EUPS dispute resolution service to address privacy complaints against U.S. companies.

About BBB EU Privacy Shield

BBB EU Privacy Shield was created by the Council of Better Business Bureaus in 2016 as a successor program to BBB EU Safe Harbor (formerly BBB Online), which was one of the original independent recourse mechanisms created to support the U.S.-EU Safe Harbor Framework in 2000. The new program pro-vides compliance assistance for U.S. companies preparing for Privacy Shield self-certification, and offers an independent third-party dispute resolution mechanism to European Union (EU) and Swiss individuals with privacy com-plaints against participating companies alleging violations of the Privacy Shield Principles. The objectives of this self-regulatory program are to ensure that privacy concerns of individual complainants are addressed expeditiously and fairly, and to promote privacy accountability among companies participating in the program. Launched July 12, 2016, the program has provided services to more than a thousand businesses of all sizes and types during its first two years of operation. Businesses seeking information about BBB EU Privacy Shield membership, and individuals with questions about privacy dispute reso-lution should visit bbb.org/EU-privacy-shield.

About BBB

For more than 100 years, Better Business Bureau has been helping people find businesses, brands and charities they can trust. In 2017, people turned to BBB more than 154 million times for BBB Business Profiles on more than 5.5 million businesses and 3.4 million times for BBB Wise Giving Alliance Charity Reports; and the BBB system handled more than 820,000 complaints across North America, free to consumers at bbb.org. The Council of Better Business Bureaus, located in Arlington, Virginia, is the umbrella organi-zation for the local, independent BBBs in the United States, Canada and Mexi-co. It is also home to national self-regulation programs addressing important business issues including online privacy and data protection, industry-specific consumer dispute resolution, and advertising truth and accuracy.

Council of Better Business Bureaus, Inc. | 3033 Wilson Boulevard, Suite 600, Arlington, VA 22201

BBB