# CLIENT ALERT – EU-U.S. PRIVACY SHIELD PROGRAM OPEN FOR SELF-CERTIFICATION

- Self-certification for the new EU-U.S. Privacy Shield started August 1, 2016.
- The Privacy Shield is a voluntary program for compliance with EU laws restricting the transfer of personal data from the EU to the U.S. If you choose not to self-certify, you will need to use an alternate method to lawfully transfer EU personal data (e.g. model clauses, or binding corporate rules). It replaces the much simpler (but now invalidated) EU-U.S. Safe Harbor program.
- If your business receives personal data from within the EU (either directly from individuals or indirectly from other businesses), you should evaluate whether to self-certify under the Privacy Shield.
- The Privacy Shield will require you to comply with substantive restrictions on collection and use of data, update your privacy policy, enter into new agreements with your subcontractors, and participate in dispute resolution and compliance reporting regimes.
- Due to the operational and legal requirements of the Privacy Shield, and the increased risk of enforcement compared to its predecessor Safe Harbor program, you will need to consider participation carefully as part of a larger global data privacy plan.
- We recommend that you consult with your attorney in the Gunderson Dettmer IP group to discuss your options in more detail. Gunderson Dettmer currently has over 35 lawyers addressing privacy and data security issues, including over a dozen Certified Information Privacy Professionals ("CIPPs").

## What is the EU-U.S. Privacy Shield?

The new EU-U.S. Privacy Shield program opened for self-certification on August 1, 2016. The program was designed by the U.S. Department of Commerce and the European Commission to provide EU and U.S. companies with a mechanism to comply with EU data protection requirements when transferring personal data from the EU to the U.S. It replaces the EU-U.S. Safe Harbor program which was invalidated by the EU Court of Justice in October 2015.

The Privacy Shield, which contains significantly more onerous terms than its predecessor Safe Harbor program, is designed to provide appropriate safeguards for data transfers under both existing EU data protection laws and the tougher new EU General Data Protection Regulation (GDPR). The GDPR becomes effective in May 2018 and will apply to all foreign companies processing personal data of EU residents. The Privacy Shield involves a detailed set of requirements based on privacy principles such as notice, choice, access and accountability for onward transfer, as well as stricter oversight and enforcement mechanisms for certified companies, and greater consequences for non-compliance.

The Privacy Shield program is a voluntary program. However, once an eligible company certifies under the Privacy Shield, such commitment becomes enforceable under U.S. law by the Federal Trade Commission

(FTC) or the U.S. Department of Transportation (DOT) (depending on which agency has jurisdiction). The certification must be renewed annually or it will lapse. Even if you withdraw from the Privacy Shield or let your certification lapse, you must annually affirm your commitment to continued compliance with the Privacy Shield principles with respect to (and for as long as you retain) any data collected under the Privacy Shield. The FTC has indicated that it will prioritize investigation into compliance issues raised by the Department of Commerce and the European Data Protection Authorities (DPAs) and, accordingly, we expect to see increased enforcement of non-compliance by both the FTC and the DOT.

## Should you participate in the Privacy Shield?

Since the operational and legal implications of certifying under the Privacy Shield are significant, we advise you to carefully review your data flows and overall global data privacy plan before deciding whether the Privacy Shield is right for you. While the Privacy Shield offers the advantage of a more streamlined process compared with entering into model clauses with multiple parties for complex data flows, companies need to consider the additional requirements, oversight and enforcement that are part of the Privacy Shield program. Some factors that will be relevant to your decision include your corporate structure (do you have subsidiaries, servers or branches in the EU?), data flows (are your data flows complex or simple, directly from the end user or via a third party partner?), interaction with "data subjects" (the individuals to whom the personal data relates), your budget, and the sensitivity of data categories collected and processed.

For example, if you are a U.S.-based company collecting EU personal data directly from consumers in the EU, or if you have EU subsidiaries transferring data to a U.S. parent, the Privacy Shield may be a good option. If you have complex data flows involving international transfers to recipients outside the EU and U.S. (the Privacy Shield only covers EU-U.S. transfers), or your third party vendors, customers and partners in the EU distrust the Privacy Shield (e.g., due to uncertainty over its future validity in the EU) and require you to sign model contractual clauses for the transfer of personal data (see more on those below), the Privacy Shield may not be a good option for you.

In any case, you may find that your vendors, customers and partners require you to be Privacy Shield certified, or require that you sign up to equivalent contractual provisions if you receive personal data from a Privacy Shield certified company (even if you choose to not certify under the Privacy Shield).

Note that the Privacy Shield will likely be subject to challenge in EU courts, and risks being invalidated pursuant to such challenge. If you agree to contractual Privacy Shield requirements and obligations in your third party contracts and the program is later invalidated, you will be contractually required to continue to comply.

## What do you need to do to certify?

Eligible companies can sign up on the https://www.privacyshield.gov website. You will need to pay an annual fee based on your company's annual revenue, which scales from $250 for companies with annual revenue under $5 million, up to $3,250 for companies with annual revenue over $5 billion.

Adherence to the Privacy Shield requires significant review of (and likely changes to) your internal and public-facing policies and procedures. While you will need to review the requirements of the Privacy Shield

in detail in order to self-certify, the following is a summary of key steps a certifying organization will need to take:

- Update your public-facing privacy policy to comply with the various requirements under the notice principle, and include all the required provisions under the Privacy Shield;
- Review, and if necessary amend, your contracts with partners, vendors and customers to ensure they include provisions required for Privacy Shield certified companies;
- Create internal policies to comply with Privacy Shield principles, and consider whether your product/service is designed to support compliance. For example, you must consider how your organization will handle requirements around data subjects' choices (including opt-out mechanisms where required by the Privacy Shield), data subjects' access requests, data retention/deletion, and complaints handling;
- Sign up with an independent recourse dispute resolution mechanism (EU Data Protection Authorities (DPAs) or a third party dispute resolution provider); and
- Conduct annual compliance assessments and re-certify annually.

If you certify under the Privacy Shield in the first two months following its release, you will have nine months from the date of certification to bring your existing contracts into complete conformity.

The Privacy Shield program is subject to an annual review procedure and future changes are likely. It is your responsibility as a certified company to keep up to date on such changes and ensure that you can comply. Note that you will be obligated under the upcoming GDPR with respect to the collection and processing of EU personal data whether or not you sign up for the Privacy Shield.

For more detailed information on the requirements of the Privacy Shield, see the links under "Additional Resources" below or contact us. We can help you explore whether the Privacy Shield is the right option for you, and we can refer you to third party consultants to cost-effectively assist with the mechanical aspects of certification.

## What are the consequences of non-compliance with the Privacy Shield for a company that is Privacy Shield certified (a "participating company")?

Participating companies in the U.S. are required to have in place an independent recourse mechanism to investigate and resolve privacy complaints from EU individuals (at no cost to the individuals). Sanctions the independent recourse mechanism may impose include publicity for findings of non-compliance, requirements to delete the data, suspension and removal of the Privacy Shield seal, injunctive relief and compensation to individuals for losses incurred as a result of non-compliance. If the participating company fails to comply with such sanctions, the independent recourse mechanism must notify the relevant EU or U.S. governmental body with jurisdiction, and the U.S. Department of Commerce. EU citizens may also seek enforcement through their DPA, which may submit complaints to the FTC or the Department of Commerce. If a complaint cannot be resolved through these mechanisms, U.S. companies will have to submit the complaint to binding arbitration.

The FTC can enforce non-compliance with the Privacy Shield under the FTC Act as a deceptive trade practice (this does not require a complaint from an individual) and can prohibit misrepresentations through

administrative orders or by seeking court orders. Violations of such administrative orders can lead to civil penalties of up to $40,000 per violation or $40,000 per day of continuing violations.

What are some alternatives to the Privacy Shield?

Alternative means of compliance with the restrictions on transfers of personal data from the EU to the U.S. include:

Keep the data within the EU: This may be an option for some companies that are able to set up separate servers or a cloud with geographic restrictions. Some cloud service providers offer EU-specific clouds, but note that if you access the data from the U.S. (e.g., through remote access in the course of providing support), that still constitutes a transfer from the EU, so this method may be impractical for many companies.

Model Clauses: These are standard contracts approved by the European Commission. Except for a few optional provisions, the provisions cannot be amended (and will lose their pre-approved status if amended). There are currently three sets of model clauses (2001 Controller-Controller, 2004 Controller-Controller, and 2010 Controller-Processor). (A "data processor" is the party that processes the personal data on behalf of, and according to the instructions of, the data controller. The "data controller" is the party that determines the purposes for which and the manner in which any personal data is processed. "Processing" is broadly defined and covers almost any activity taken with respect to the data, such as collecting, storing, transmitting, and even deleting the data.)

The model clauses will be a good compliance option in some situations, but they are inflexible (in particular where there are complex and changing data flows) and the exposure to audit is greater than under the Privacy Shield. The model clauses require that you submit to the jurisdiction of the data protection authority in the EU member state where the data exporter is located, and you may be audited by that authority and by the data exporter. Additionally, the data subject is given third party beneficiary rights.

Further, the model clauses for data processors (often the applicable contract for companies providing services) require the data controller's prior approval for subprocessing and the data processor must flow down the same model provisions to its subprocessors, which is a concern for many companies. The Privacy Shield is more flexible regarding the use of subprocessors, and while equivalent contractual protections are required in contracts between a Privacy Shield certified company and a subprocessor, verbatim flow-down terms and prior consent of the data exporter are not required under the Privacy Shield.

Ad Hoc Contracts: Companies can enter into individually negotiated ad hoc contractual arrangements (that do not need to be on the prescribed form of the model clauses). However, such contracts will need to be filed with and approved by the relevant EU data protection authorities prior to the transfer, and must be consistent with legal data protection principles.

Binding Corporate Rules: More large companies are working on establishing Binding Corporate Rules (BCRs). BCRs are a global code of practice based on EU privacy standards, are mostly used by large multinational companies with complex data flows, and are a mechanism to legitimize data exports within a corporate group. There are also BCRs for data processors. BCRs require approval by the data protection

authorities in the designated EU member states. The BCRs may be a good option if you are concerned with data flows within a large multinational company.

Alternatives that we generally do not recommend:

Consent from EU data subjects: Consent is difficult to use because Europeans consider consent to require compliance with a broad bundle of rights. Under European law, consent must be freely given, specific, informed, and unambiguous, and one must be able to withdraw consent with the effect that further processing of collected data ceases. Further, consent is invalid if the data subject is not given a real choice. Since EU authorities do not consider "consent" given by an employee to an employer to be freely given, consent is not an effective option for employee data.

Relying on derogations: "Necessary" transfers are one of a few narrow exceptions ("derogations") to the EU restriction on data transfers that some companies have tried to take advantage of. These efforts have largely been unsuccessful because the scope of "necessary" transfers has been construed very narrowly. In order to qualify, (a) the transfer must genuinely be necessary for some narrowly defined legitimate purpose (such as for performing a contract in the interest of the data subject) and (b) if the transfer is not directly from the data subject, the transfer must be pursuant to a contract entered into at the data subject's request or in his/her interest and must be necessary for the performance of that contract.

Additional Resources

International Trade Administration Privacy Shield Website:
https://www.privacyshield.gov

Full text of the Privacy Shield available for download:
https://www.privacyshield.gov/EU-US-Framework

Department of Commerce Privacy Shield Website:
https://www.commerce.gov/privacyshield

Department of Commerce FAQs:
https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/faqs-eu-us_privacy_shield_7-16_sc_cmts.pdf

Department of Commerce Fact Sheet:
https://www.commerce.gov/news/fact-sheets/2016/07/fact-sheet-overview-eu-us-privacy-shield-framework

If you have any questions regarding the matters covered in this client alert, you may contact any of the authors of this alert listed below:


| | | |
|---|---|---|
| Anna Westfelt | 650-463 5367 | awestfelt@gunder.com |
| Katherine Gardner | 212-430 3188 | kgardner@gunder.com |
| Gina Marek | 650-463 5242 | gmarek@gunder.com |


You may also contact your regular Gunderson Dettmer attorney or any of the following privacy and data security contacts:


| | | |
|---|---|---|
| Colin Chapman | 650-463 5490 | chapman@gunder.com |
| Tom Villeneuve | 650-463 5460 | tvilleneuve@gunder.com |
| Aaron Rubin | 212-430 3181 | arubin@gunder.com |
| Aaron Fiske | 650-463 5443 | afiske@gunder.com |
| Marna Pattaropong | 617-648 9299 | mpattaropong@gunder.com |
| Peter Schoch | 617-648 9233 | pschoch@gunder.com |
| David Sharrow | 212-430 3161 | dsharrow@gunder.com |