ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

GDPR and Privacy Shield: Different Tools for Different Goals

Compliance and Ethics

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Privacy Shield.*** The EU-US Privacy Shield is a cross-border data transfer mechanism, not a data protection law or a comprehensive data protection compliance framework.
- ***Important differences.*** GDPR is significantly broader, deeper, and more specific than the Privacy Shield.
- ***Regardless of geography.*** Even if a company does not do business in the European Union or the European Economic Area, it may be subject to GDPR because their practices include the collection, processing, or monitoring of personal data of individuals located in the European Union.
- ***Not an either/or situation.*** Organizations cannot meet their obligations under GDPR solely through a self-certification of their commitment to observe the Privacy Shield principles.

US-based organizations are realizing that they must comply with the EU General Data Protection Regulation (GDPR) — even if they do not do business anywhere in Europe — because their practices include the collection or processing of personal data of individuals located in the European Union or the monitoring of their activities. Unlike its predecessor — Directive 95/46/EC, known as the EU Data Protection Directive — GDPR was drafted to apply to many organizations established outside the European Union, so that the protection follows the data when it is moved or processed abroad.

GDPR Article 3 is the key provision regarding the territorial reach of the GDPR. Under Article 3(1), the GDPR applies to the processing of personal data in the context of the activities of the establishment of an entity in the European Union. In practice, the protection extends to individuals located in Norway, Iceland, and Lichtenstein, because, like most laws of the European Union, GDPR is incorporated into the laws of these three countries, and thus its scope covers the entire European Economic Area (EEA), which is comprised of the European Union and these three additional countries.

Article 3(2) extends the territorial scope of GDPR outside the EU or EEA borders. It states that GDPR applies to the processing of personal data of individuals who are in the European Union/EEA by a data controller or processor established outside the European Union/EEA, when the processing is related to the offering of goods or services to such individuals or the monitoring of their behavior. Article 3(2) attaches to numerous US entities and requires them to comply with the entire GDPR.

Some organizations assume that it is enough for them to have self-certified their adherence to the EU-US Privacy Shield (Privacy Shield) and that their self-certification is sufficient to address all 99 articles of the GDPR. This is incorrect. While the Privacy Shield and GDPR overlap in some areas, GDPR is much broader and contains many more requirements.

This article compares the Privacy Shield and GDPR, to highlight commonalities, but also gaps that organizations need to address to achieve compliance under both frameworks.

Background

The EU-US Privacy Shield framework is a cross-border data transfer mechanism, which relies on the Privacy Shield Principles and Supplemental Principles (collectively Shield Principles). It was developed in consultation between the US Department of Commerce and the European Commission, and finalized in July 2016. It addresses the restrictions to the transfer of personal data outside the European Union or EEA under Articles 44-50 of GDPR (and before that, Articles 25-26 of the EU Data Protection Directive 95/46/EC). These provisions require the data exporter to ensure that EU or EEA data subjects will continue to benefit from effective safeguards and protection after their data has been transferred outside the European Union or EEA. This assurance can be provided through different means. The EU-US Privacy Shield framework is one of these means of providing the assurances required by GDPR Articles 44-50.

The Privacy Shield framework was not drafted to meet the requirements of GDPR or as an alternative to GDPR. It was drafted separately from GDPR; it is not even mentioned in GDPR. The Privacy Shield Principles meet only a small aspect of GDPR. The Shield is limited to providing a legal ground for the processing of EU or EEA data in the United States establishing for EU or EEA individuals and regulators a means for reaching US-based organizations in the United States and initiating enforcement. It is a data transfer mechanism only. It also addresses some concerns regarding access by US national security to EU or EEA data stored in the United States; this aspect of the Privacy Shield framework is not discussed here.

Common elements of the Privacy Shield Principles and GDPR

There are similarities and, at times, overlap between the Shield Principles and GDPR. The latter is significantly broader, deeper, and more specific than the Shield Principles. In this section, we look at the seven basic Principles of the EU-US Privacy Shield and compare them with the equivalent provisions found in the GDPR.

1. Notice

The Notice Principle requires an organization, among other things, to inform individuals about its commitment to process all personal data received from the EEA in compliance with the Privacy Shield Principles and in reliance upon the Shield; the fact that the organization is subject to investigatory and enforcement powers of the Federal Trade Commission or the US Department of Transportation; the requirement to disclose personal data in response to lawful requests; the possibility of invoking binding arbitration; how to contact the organization with inquiries and complaints; and the independent dispute resolution body designated to address such complaints.

An organization must also inform individuals of the types of personal data collected; the purposes for which it collects and uses personal data about them; the individuals' rights to access their data; the choices and means the organization offers them to limit the use and dissemination of their personal data; the identity of third parties to which the data is disclosed; and the organization's liability in cases involving transfer to third parties.

Most of these requirements are found in GDPR Article 5(1) (a) [Lawfulness, Fairness, and Transparency] and GDPR Article 5(1(b) [Purpose Limitation]. They are further detailed in GDPR Art. 12 [Transparent information], Art. 13 and 14 [Information to be Provided], among others.

2. Choice

Under the Choice Principle, an organization must offer individuals the opportunity to opt out of having their personal data disclosed to a third party or used for a purpose materially different from the purpose for which it was originally collected. It is unnecessary to provide choice when the disclosure is made to a third party acting as an agent of the organization. However, the organization must enter into a contract with the agent.

For sensitive information (medical or health conditions, information specifying the sex life of the individual, racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership), organizations must obtain the individual's express affirmative consent before such information is disclosed to a third party or used for a purpose that is materially different than the purpose for which it was originally collected.

> Under the Choice Principle, an organization must offer individuals the opportunity to opt out of having their personal data disclosed to a third party or used for a purpose materially different from the purpose for which it was originally collected.

Most of these requirements are found in GDPR, for example in Articles 6(4) [Lawfulness of the Processing, 7 [Conditions for Consent], 9 [Special Categories of Data] as well as GDPR Article 5(1)(a), [Lawfulness, Fairness, and Transparency] and Article 5(1(b) [Purpose Limitation].

The Choice Principle requires offering individuals the opportunity to opt-out from the disclosure of their personal data to a third party or the use of the data for a materially different purpose than the one originally announced. GDPR Article 21 [Right to Object] grants individuals the right to object to the use of personal data for the legitimate interest of the data controller and to the use of personal data for marketing purposes.

Notably missing from the Privacy Shield framework are the rights of EU or EEA citizens not to be subjected to automated decision-making, including profiling, found in GDPR Article 22(1) and the right to restrict the processing of their personal data, such as when it is contested or no longer needed, found in GDPR Article 18(1).

3. Accountability for onward transfer

To transfer personal data to a third party acting as a data controller, organizations must comply with the Notice and Choice Principles and enter into a contract with the controller. The contract must specify that personal data may only be processed for limited and specified purposes consistent with the consent obtained from the individual. The contract must also specify that the recipient will provide the same level of protection as the Shield Principles and will notify the organization if it can no longer meet this obligation and take reasonable steps to remediate.

To transfer personal data to a third-party agent, organizations must transfer the personal data only for limited specified purposes and ensure that the agent provides at least the level of protection required by the Shield Principles. They must take reasonable and appropriate steps to ensure that the agent effectively processes the personal data transferred in a manner consistent with the organization's obligations under the Shield Principles. They must also require the agent to notify the organization if it can no longer comply with the Principles and must take reasonable steps to remediate unauthorized processing.

Under GDPR, when a US-based data controller wishes to transmit data to a data processor located

outside the European Union or EEA, two sets of provisions apply. GDPR Article 28 deals with the use of a processor. GDPR Articles 44 and 46 address the adequacy of the safeguards to be provided by the foreign entity; these provisions focus on cross-border data transfers and further transfers to third parties and are consistent with the Shield Onward Transfer Principle.

The comprehensive GDPR Article 28 outlines in detail the required content of the contract between the controller and the processor. For example, the contract must stipulate that the processor may process the data only on documented instructions of the controller; must assist the controller in responding to data subjects' exercise of their rights; must obtain the controller's consent before enrolling a subcontractor; and must notify the controller if the controller's instructions would infringe applicable law.

4. Security

The Security Principle requires organizations that self-certify compliance with the Shield to take reasonable and appropriate measures to protect personal data from loss, misuse, unauthorized access, disclosure, alteration, or destruction. GDPR Article 5(1)(f) [Integrity and Confidentiality] also requires organizations to ensure appropriate security of the personal data. GDPR Article 32 [Security of Process] provides additional parameters for the identification and choice of security measures, including a number of specific security measures that organizations must undertake when handling personal data originating from the European Union or EEA.

The Shield Principles do not deal with the impact of security breaches. While the Security Principle requires the use of appropriate measures to protect data from loss, misuse, unauthorized access disclosure, alteration, or destruction, it does not address the potential effect of a security incident or require any form of notice to supervisory authorities or affected data subjects.

> The Shield Principles do not deal with the impact of security breaches.

On the other hand, GDPR Articles 33 and 34 detail with great specificity the actions to be taken in the event of a data breach. Among those, the affected data controller must notify the supervisory authority or authorities within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedom of individuals. They must also notify individuals "without undue delay" if the breach is likely to result in a high risk to the rights and freedoms of the individuals.

Data processors who suffer a data breach must notify the controller without undue delay after becoming aware of the breach. Further, GDPR Article 28(3)(c) and Article 28(3)(f) flow down these requirements to processors and their own subprocessors.

5. Data integrity, purpose, retention

The Shield Principles require that the collection of personal data be limited to what is relevant for the purposes of processing. An organization must take reasonable steps to ensure that personal data is reliable, accurate, complete, and current, and it must retain the data in a form that makes the individual identifiable only for as long as is reasonably necessary to serve the purpose for which it has been collected and to which the individual has consented.

GDPR Article 5(1)(b) [Purpose Limitation], GDPR Article 5(1)(e) [Storage Limitation], and GDPR

Article 5(1)(f) [Integrity and Confidentiality] cover similar issues.

6. Access

The Access Principle grants individuals the ability to have access to personal data about them that an organization holds. They are also able to request the amendment or deletion of information that is inaccurate or was collected in violation of the Privacy Shield Principles.

The scope of the rights of individuals under the GDPR is much greater; it extends beyond the right of access, correction, or deletion. Article 20 provides the right to data portability, while Article 21 [Right to Object], includes, for example, the right to object to certain uses of personal data and the right to object to the use of personal data for marketing purposes. GDPR Article 22 [Automated Individual Decision-Making] grants the right not to be subject to a decision solely based on automated processing.

The right of erasure, under GDPR Article 17, is also more complex and more nuanced. The Privacy Shield limits the right of deletion to situations where the data is inaccurate or was collected in violation of the Shield Principles. GDPR right of erasure or “right to be forgotten” provides for the right to have data deleted when the individual withdraws consent on which the processing is based, if there are no other legal grounds for the processing. It also includes a provision for the deletion of data about children that has been collected in connection with the use of internet services.

7. Recourse, enforcement, and liability

Both the Shield Principles and GDPR require organizations to have mechanisms in place for ensuring compliance with the applicable rules. In the Privacy Shield, the Recourse Principle requires the use of independent recourse mechanisms (such as the American Arbitration Association or the Better Business Bureau). The mechanisms must be readily available at no cost to the individual. The recourse mechanism also must allow for the award of damages in accordance with applicable law or the rules of the recourse mechanism. There must be follow-up procedures for verifying the accuracy of the assertions made by organizations about their data protection practices. Furthermore, organizations must respond promptly to requests from the Department of Commerce for information related to the Privacy Shield and to complaints referred by EU/EEA Member State supervisory authorities through the Department of Commerce.

> In addition to the independent recourse mechanisms, violation of the Shield Principles, or misrepresentation as to compliance with them, may be subject to investigations by the Federal Trade Commission (FTC).

In addition to the independent recourse mechanisms, violation of the Shield Principles, or misrepresentation as to compliance with them, may be subject to investigations by the Federal Trade Commission (FTC). When an organization becomes subject to an FTC or court order based on noncompliance, it must make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Recourse and Enforcement Principle allows affected individuals to bring their complaints directly within the purview of US-based enforcement authorities, private or governmental, which might make enforcement easier, faster, and more effective. The Recourse and Enforcement Principle does not identify specific administrative fines. FTC consent decrees issued after investigations of non-compliance with the Shield Principles have included significant obligations, such as record keeping

requirements for 20 years after the issuance of the order, which can present a significant financial burden, among other things.

GDPR Articles 77 to 84, on the other hand, provide extensive remedies and significant fines. Individuals have the right to lodge a complaint with a Supervisory Authority, under GDPR Article 77, and the right to judicial remedy in the courts of the Member State where the individual resides, under GDPR Article 79. Individuals can also mandate a nonprofit organization to lodge a complaint on their behalf, under GDPR Article 80, and may receive compensation, under GDPR Article 82 [Right to Compensation]. Most important, GDPR Article 83 [Administrative Fines] allows for the imposition of administrative fines that may reach €20 million or four percent of the total worldwide annual turner of a global entity, whichever is higher.

In the case of recourse and enforcement under GDPR, it remains to be seen how EU or EEA authorities and courts will be able to assert jurisdiction or to enforce judgments, damages, or fines over organizations located outside the European Union or EEA. GDPR Article 27 requires non-EU or EEA controllers and processors to appoint a representative located in the European Union or EEA. The representative can be addressed in addition to, or instead of, the controller or processor by supervisory authorities and data subjects for ensuring compliance with GDPR. GDPR Recital 80 indicates that the designated representative could be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

> In the case of recourse and enforcement under GDPR, it remains to be seen how EU or EEA authorities and courts will be able to assert jurisdiction or to enforce judgments, damages, or fines over organizations located outside the European Union or EEA.

At this time, there is little clarity on how enforcement proceedings could be conducted and what the potential outcomes might be. Would the role of the representative be limited in most cases to that of an agent for receiving communications and providing responses, or could the representative become jointly and severally liable with the non-EEA entity? GDPR Article 27 is silent, and, so far, no guidelines have been issued. In addition, it is also not clear how a judgment rendered in the European Union or EEA against an organization established abroad would be enforced.

When addressing recourse and enforcement, GDPR and Privacy Shield adopt different routes and pertain to different subject matters. Privacy Shield focuses on enforcement of the violation of the Privacy Shield Principles in the United States, where the FTC is likely to have a significant role in stopping a US company from conducting non-compliant activities, and historically has been a tough enforcer.

GDPR focuses on enforcement in the European Union or EEA, pertains to the entire GDPR, provides local government agencies with the ability to assess significant fines, and grants individuals a private right of action to seek damages. In the past, EU or EEA agencies have not been as aggressive as their US counterparts, but the landscape is likely to change with the significant fines available under GDPR Article 83.

It remains to be seen what will happen in practice, which of these avenues will be more frequently used in the event of a dispute, what the outcome of enforcement action will be, and which mechanism will provide more effective enforcement or recourse for affected individuals or create more barriers or hurdles for organizations.

GDPR concepts that are not addressed in the Shield Principles

In the first part of this article, we showed that in six of the areas covered by the Shield Principles the GDPR takes a more comprehensive view and contains more stringent, detailed, and specific requirements. The seventh Shield Principle, enforcement, differs significantly from the enforcement provisions of the GDPR. Given that enforcement of the Shield Principles has been limited to a handful of FTC actions, it is difficult to make a practical comparison between the two enforcement mechanisms at this time.

When we move the analysis and the comparison to other areas, it becomes even clearer that a self-certification of adherence to the Shield Principle is insufficient to show compliance with all GDPR provisions that may be applicable to organizations. We provide several examples below:

1. Legal grounds for processing data

The Privacy Shield Notice and Choice Principles require organizations to disclose the purpose of collecting personal data and obtain consent to conduct certain activities, such as disclosure to third parties or use for a purpose materially different from the originally disclosed purpose. However, it assumes, *a priori*, that the data have been legally collected or that the consent was implied from the conduct of the parties.

GDPR Article 6 (1) requires that the collection and processing of personal data be lawful. It identifies only six limited grounds for collection and processing to be legal. For example, processing will be lawful if it is necessary for the performance of a contract to which the data subject is a party or to comply with a legal obligation. Processing will also be lawful if it is conducted for the legitimate interests of the controller or a third party, so long as these interests are not overridden by the fundamental rights and freedoms of the individual. In some cases, a data controller may have no other choice than seeking and obtaining the explicit consent of the individual (opt-in consent) to provide the required legal basis for the contemplated processing.

2. Obligations regarding data subject rights

In addition to providing extensive rights to individuals located in the European Union or EEA, GDPR imposes obligations on data controllers to facilitate the exercise of those rights. Controllers must provide individuals with information about their rights as data subjects and must facilitate the exercise of those rights electronically. Controllers must respond to a data subject’s request within one month and provide information on actions taken or not taken in response to a request. In addition, data processors are contractually required to cooperate with the data controller to address such rights.

3. Data protection by design and default

GDPR Article 25 [Data Protection by Design and by Default] requires data controllers to implement appropriate measures to ensure that the processing implements the data protection principles. It also requires that the processing meet the GDPR principles and requirements, assure and protect the rights of the individual, and that, by default, the processing be limited to the personal data necessary for a specific purpose.

4. Documentation of processing and data protection impact assessment

GDPR Article 30 [Record of Processing Activities] requires controllers and processors to keep electronic records of their processing activities, to be made available to supervisory authorities upon request. When processing activities are likely to result in a high risk for the rights and freedoms of individuals, GDPR Article 35 [Data Protection Impact Assessment] requires data controllers to assess the impact of the envisaged processing on the protection of personal data. Both Articles 30 and 35 are likely to have a significant operational impact on organizations.

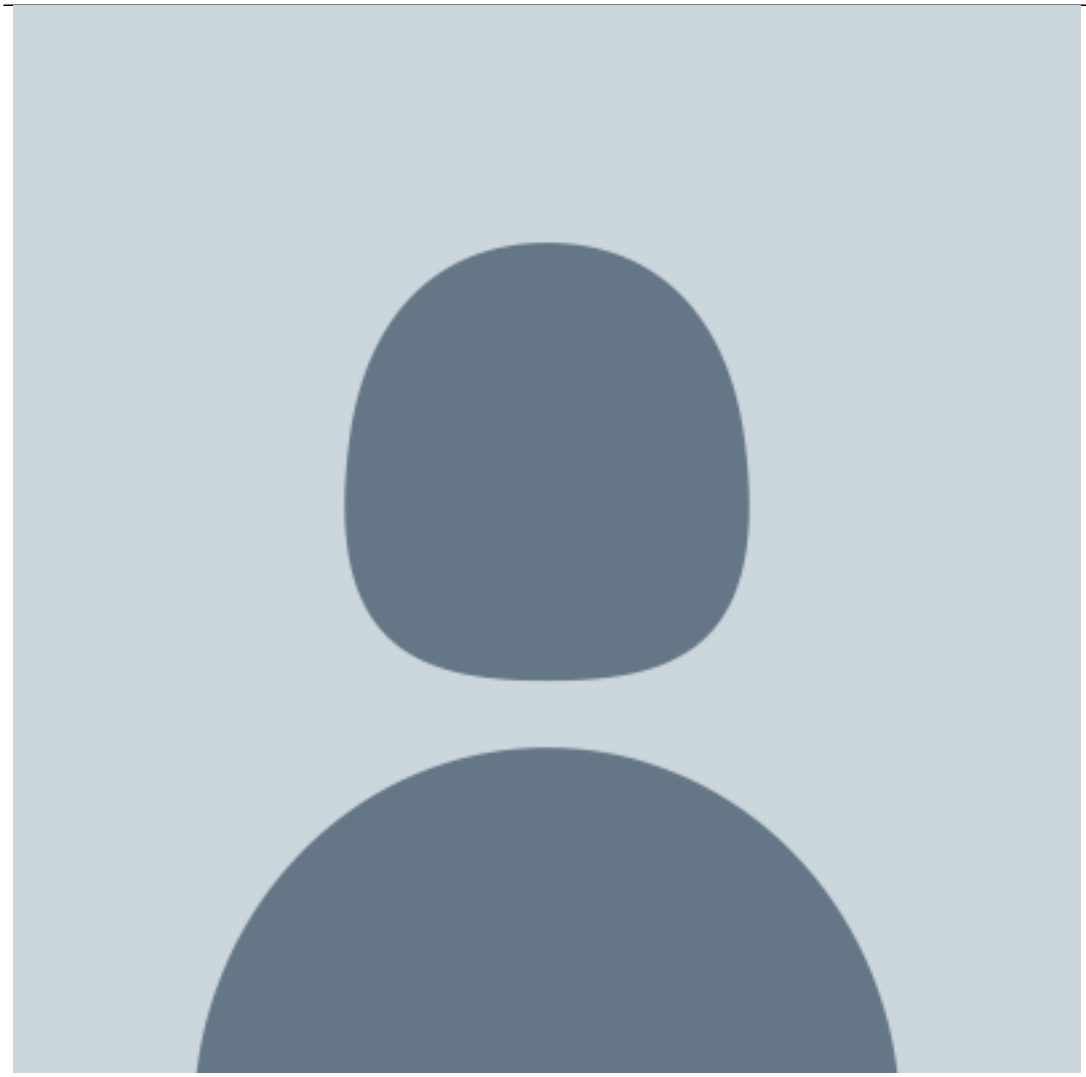
Conclusion

Even if a company does not do business in the European Union or the EEA, it may be subject to GDPR. Compliance with GDPR requires significant efforts, time, and financial investments.

The Privacy Shield Principles provide a simple, easy-to-use means for organizations to address their obligations under Chapter V, Articles 44-50 of the GDPR [Transfer of Personal Data to Third Countries or International Organizations]. However, the use of the Privacy Shield just serves its original purpose: providing a means for US entities to show their commitment to protecting personal data originating in the European Union or EEA when the processing is conducted in the United States and to respond to complaints and enforcement actions that may be initiated in the European Union or EEA and subsequently transmitted to US agencies. The Privacy Shield is not a data protection law or a comprehensive data protection compliance framework. It is a cross-border transfer mechanism.

As both the Privacy Shield and GDPR are further explained and clarified, organizations should understand the narrow, limited, and specific role of the Privacy Shield, the significant gaps between the Privacy Shield and GDPR, and that they cannot meet their obligations under GDPR solely through a self-certification of their commitment to observe the Privacy Shield principles.

Paola Zeni



Senior Director of Global Privacy

Palo Alto Networks

Francoise Gilbert

Shareholder

Greenberg Traurig LLP

She focuses her practice on global data privacy and cybersecurity.

Max Calehuff

Attorney in the Cybersecurity and Privacy Group

Greenberg Traurig LLP