When our client was hacked, we had to react swiftly and with precision. And this is exactly why we rely on Bloomberg Law. Its news and unique analytics keep us ahead of fluid domestic and global privacy and data security laws, as well as the latest trends in managing breaches. We were able to quickly advise on how to respond, report and comply. Bloomberg Law. Because reaction time matters.

www.bna.com/bloomberglaw
U.S. companies that do business in the EU or transfer personal data outside of the EU are facing challenging times. Compliance with the first major revamp of the bloc’s privacy framework in over 20 years—the General Data Protection Regulation (GDPR)—is on the near horizon. The Safe Harbor agreement between the U.S. and EU, which allowed over 4,000 U.S. companies and tens of thousands of EU companies to legally carry out data transfers, was tossed. The Privacy Shield proposed to take Safe Harbor’s place faces skepticism and possible legal challenges. And the echoes of Edward Snowden’s disclosures continue. With the effective date for the landmark GDPR now set as May 25, 2018, companies and organizations have 18 months from the date of this session to get their corporate ducks in a row. The stakes are high, with fines that could be as much as 4 percent of a company’s worldwide turnover or $20 million euros, whichever is higher. Here, we will discuss the essentials of GDPR compliance and what U.S. companies must be most concerned with to ensure they meet EU data transfer requirements.

<table>
<thead>
<tr>
<th>EU GENERAL DATA PROTECTION REGULATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special Report: New EU Privacy Law Has Tougher, but More Coherent Fines</td>
</tr>
<tr>
<td>Special Report: High-Risk Processing Triggers EU Data Reg Obligations</td>
</tr>
<tr>
<td>Bloomberg Law Insights: EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EU-U.S PRIVACY SHIELD</th>
</tr>
</thead>
<tbody>
<tr>
<td>The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options</td>
</tr>
<tr>
<td>Bloomberg Law Insights: Concrete Solution, or Are the Sands Still Shifting? European Data Protection Post- Schrems</td>
</tr>
<tr>
<td>EU Certificate May Be U.S. Data Transfer Alternative</td>
</tr>
<tr>
<td>Bloomberg Law Insights: Impact of the EU-U.S. Privacy Shield on Health-Care Data Transfers</td>
</tr>
<tr>
<td>Special Report: New EU-U.S. Data Transfer Pact May Face Court Challenges</td>
</tr>
<tr>
<td>Bloomberg Law Insights: EU-U.S. Privacy Shield 2.0 Signed, Sealed and Delivered</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BREXIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bloomberg Law Insights: Brexit's Impact on International Data Transfers</td>
</tr>
<tr>
<td>Special Report: Brexit Sparks EU Single Market Privacy Conundrum</td>
</tr>
<tr>
<td>Special Report: Companies Should Focus on EU Privacy Regime Post-Brexit</td>
</tr>
</tbody>
</table>
New EU Privacy Law Has Tougher, but More Coherent Fines

**BNA Snapshot**

**Sanctions Under EU General Data Protection Regulation**

**Development:** European Union General Data Protection Regulation will take effect May 25, 2018, ushering in new system of potential multi-million euro fines for data privacy violations.

**Takeaway:** U.S. companies should be prepared for possibility of huge fines from EU privacy regulators even if the likelihood of them being assessed feels unlikely or remote.

By Stephen Gardner

June 17 — What happens when a peashooter is suddenly replaced by a cannon? That is the question companies are asking about the huge fines that will become available under the European Union's new landmark privacy law.

After the new General Data Protection Regulation (GDPR) takes effect in May 2018 all of the privacy offices in the 28 EU countries will gain powers to levy multi-million euro fines for serious privacy infringements.

U.S. companies should be prepared for possibility of huge fines from EU privacy regulators even if the likelihood of them being assessed feels unlikely or remote, privacy attorneys told Bloomberg BNA. The new privacy law also covers a broader scope of companies than the old law making it even more important to understand the new sanctions regime, they said.

The crucial issue for companies won't be about the levels of potential fines, but how privacy regulators adapt to and exercise their new enforcement powers. For some privacy regulators, the new level of sanctions available under the GDPR will bring a dramatic change in enforcement culture, the attorneys said.

Julie Bossaert, a data protection and information security attorney with CMS DeBacker in Brussels, said that “at the moment there is a high degree of variation” in the powers of EU privacy regulators to sanction privacy breaches. Fines are “peanuts compared to what they will be,” she said.

**Millions, Even Billions of Dollar Fines Possible**

Under the GDPR, the maximum fines allowed will escalate to 20 million euros ($22.5 million) or up to 4 percent of a company's global revenues, whichever is higher. The high level fines are allowed for violations of data processing consent, individual privacy rights, international data transfer rules and ignoring orders from privacy regulators.

To put the sanctions tied to worldwide revenue in context, 4 percent of Facebook Inc.’s worldwide revenue would be approximately $500 million and 4 percent for Walmart Stores Inc. would be over $19.5 billion.

For other lesser infringements, the GDPR will allow maximum fines of the higher of 10 million euros ($11.25 million) or 2 percent of global revenues. Infringements in this bracket include failure to notify data security breaches, failure to implement preventative measures, failure to correctly maintain records and breaches over the obtaining of consent for the processing of children’s data.
Massive New Powers for Some Regulators

How data privacy regulators acclimate to their new enforcement powers is uncertain. Companies may have reason to worry.

Although the GDPR is a single law covering all of the 28 EU countries, enforcement of the privacy rules will continue to take place at the individual country level. National data protection authorities will be responsible for overseeing companies that use personal data that have their “main establishment” in the country.

For many privacy regulators, the new sanctioning powers will be a massive leap.

Bulgaria’s Commission for Personal Data Protection, for example, can levy a maximum fine of about $57,500. Ireland’s Office of the Data Protection Commissioner has no power to impose fines, although it can refer enforcement actions to a court, which may impose fines of up to 100,000 euros ($112,500).

Regulatory Muscle Flexing?

A concern for companies doing business in the EU is that the sudden increase in fining power for privacy regulators may encourage some to flex their muscles and seek to set a benchmark of tough enforcement.

Frédéric Louis, a data protection partner with WilmerHale in Brussels, warned of the possibility of a rapid ratcheting up of fines.

Fines are “one easy metric for everyone to follow,” Louis said. “As soon as one breaks ranks and imposes a big fine, immediately the others will want to” do the same.

As soon as one EU country data privacy regulator “breaks ranks and imposes a big fine, immediately the others will want to” do the same.

Frédéric Louis, Partner, WilmerHale, Brussels

CMS DeBacker's Bossaert said the new law will also in principle allow privacy regulators to levy large fines at an earlier stage of enforcement proceedings.

Martin Fanning, an information technology, intellectual property and data protection partner with Dentons in London, said the potential for high fines has turned data protection into a “top-table board-level issue,” he said.

Likelihood of High Fines Uncertain

WilmerHale’s Louis said companies looking to gauge whether privacy
Regulators will pounce to levy fines may want to look to antitrust enforcement, where the number of cases and levels of fines increased rapidly after the turn of the millennium.

In antitrust, the European Commission and the U.S. Department of Justice got into an “arms race as to who was going to impose a bigger fine.” Similar behavior among EU privacy regulators that “want to be taken seriously” might “lead to very quick development of high fines,” which would then become the norm, Louis said.

But other privacy analysts said it is more likely that EU privacy regulators will adopt a more cautious approach in exercising their new fining authority.

Bossaert said high fines would be a last resort. “I do not see, for example, the Belgian Privacy Commission imposing a fine of up to 4 percent of a company's global revenues, she said.

Alex Whalen, senior policy manager at DIGITALEUROPE, which represents information technology and consumer electronics companies, said that there remains the possibility that a particular national privacy regulator might try “to make a statement by going after a company to make an example of them.”

However, DPAs would likely be aware that rapid recourse to high fines could deter some companies from investing in the EU, Whalen said. “In general, we find most DPAs to be quite reasonable,” he added.

According to Louis, however, Article 29 Working Party had “not been a force for restraint; rather they have been a force for very strict enforcement of the rules,” and this could indicate a willingness to opt quickly for tough sanctions.

**Reach of Privacy Law Expands**

The potential kinds of companies that may face privacy fines is expanded under the new privacy regulation. Under the old law, only companies that actually controlled the use of personal data were subject to sanctions. Under the new regulation, companies that are engage in processing personal data, even though they aren't the ones that initially collected or used the data, may also be subject to fines.

Deema Freij, senior vice president with Intralinks, a provider of secure cloud services and thus a data processor, said that data processors are worried about the fines.

“This is the first time that processors have a direct compliance risk,” Freij said. Companies engaged in data processing are going back to data controller companies and asking to revisit contractual obligations, she said.

**Little Fining Experience**

High fines for privacy violations aren't completely new in the EU. The Dutch DPA, in 2014 threatened Alphabet Inc.'s Google Inc. with daily fines up to a ceiling of 15 million euros for noncompliance with DPA orders (13 PVLR 2167, 12/22/14).

The Belgian Privacy Commission in 2015 referred Facebook Inc. to a Belgian court where it received an order to stop tracking non-Facebook users or face a 250,000 euro ($282,171) penalty per day (14 PVLR 2095, 11/16/15).

Those fines, however, weren't actually enforced.

Even in EU countries where privacy regulators already have authority to impose relatively high penalties, there is limited experience of applying high fines in practice.

In the U.K., for example, the Information Commissioner's Office has the power to issue fines up to 500,000 pounds ($707,250), but the record U.K. fine so far—against Sony in 2013—was only half that amount (12 PVLR 1288, 7/22/13).

Mary J. Hildebrand, founder and chair of the Privacy and Information Security Practice at Lowenstein Sandler LLP, in Roseland, N.J., said “there's going to have to be significant guidance in terms of how those fines are levied.”
Guidance will be significant because it could influence the calculation of fines, which could either “put a damper on the process,” or lead to high fines from the outset, Louis said.

To contact the reporter on this story: Stephen Gardner in Brussels at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com
High-Risk Processing Triggers EU Data Reg Obligations

By Stephen Gardner

April 28 — When it comes to processing personal data in the European Union, companies will soon need to figure out whether it is “high risk” behavior or face significant fines.

Provisions in the forthcoming EU General Data Protection Regulation (GDPR) on data processing that involves a “high risk” to the data subject may lead multinational companies to increasingly view privacy through a European lens.

Under the GDPR, data controllers will be required to determine whether their processing operations are high risk—a determination that would trigger several obligations, including the requirement to carry out a data protection impact assessment (DPIA).

Philip James, a partner at Sheridans, a media law firm in London, said that “in assessing whether something is high risk, it's not necessarily a question of volume of data. It could be processing one data record.”

The GDPR high-risk assessment requirement could be relevant for an “innovative technology that hasn't been exploited before,” or an existing technology that is being applied to new data, James said.

Big data applications carry a “greater risk of infringing on people's privacy” and would require DPIAs under the GDPR, James said.

In addition, despite the new harmonizing regulation, each of the 28 EU member states may end up with their own definitions of what they consider to be high risk, attorneys told Bloomberg BNA.

What that all means for companies doing business in the EU is that they must carefully assess the types of data they are processing and whether they may be exposing the data subject to a risk of violating his or her fundamental rights.

Privacy Regulators' Guidance Due

The Article 29 Working Party of EU data protection officials from the 28 EU member states has promised to provide guidance on the notion of high risk and on DPIAs.

According to Ann J. LaFrance, co-leader of the data privacy and cybersecurity practice at Squire Patton Boggs LLP in London, the Art. 29 guidance can't come soon enough. While the directive mainly refers to risk as something that data controllers should take into account when deciding on data security measures, under the GDPR it “will be one of the most challenging areas,” she said.
Companies will have to be especially cautious because “this is an area that is likely to attract heavy sanctions if the new rules are not followed,” LaFrance said.

“In the event of a data breach where these rules have not been followed, the penalties and potential liability in follow-on damages claims, which are explicitly provided for in the GDPR, will likely be very substantial,” she added.

The GDPR will come into effect in mid-2018, after a two year transition period following its final approval by the European Parliament April 14 (15 PVLR 791, 4/18/16).

**Violation of Rights, Freedoms?**

High risk processing under the GDPR is considered to be processing that could impinge on the “rights and freedoms of individuals.”

These rights and freedoms are encapsulated in the Charter of Fundamental Rights of the EU, which includes both a right to protection of personal data and a right to respect for his or her private and family life, home and communications.

Erik Valgaeren, head of data protection at Stibbe in Brussels, said the protections set out in the GDPR “go to the heart of the European tradition of human rights.”

The EU has “always been out to export, these rights and freedoms,” and there is the potential for “cultural clashes,” he said.

---

Mary J. Hildebrand, founder and chair of the Privacy and Information Security Practice at Lowenstein Sandler LLP, in Roseland, N.J., said that there was the potential for misunderstanding about rights and freedoms because “you could put a dozen people in a room and they would come back with a dozen different answers on what that means.” Articles 33 and 34 of the GDPR, which set out obligations relating to the assessment of the level of data processing risk, were among the regulation’s “most challenging or at least the most vague” provisions, she said.

U.S. companies might have to work to adapt to EU norms on data privacy rights because in the U.S. there is more acceptance of “the trade-offs” between privacy and the commercial benefits from the processing of personal data, she said.

There is a “more general acceptance” in the U.S. of the use of personal data in decision-making in contexts such as
remarketing and behavioral advertising, for which in the U.S. “typically there’s no express consent” given by data subjects, Hildebrand said.

That kind of data processing “translates pretty quickly into profiling,” which would fall within the category of high-risk processing under the GDPR and “would be a prime example of something that would require an assessment” of the risk to rights and freedoms, she said.

Among companies there is a “very strong willingness to comply with the GDPR,” and “over time the additional requirements imposed by the GDPR may translate eventually into more common practice in the U.S.,” Hildebrand said.

Valgaeren said that because non-EU companies will likely assimilate EU standards on privacy freedoms and rights as they move to comply with the GDPR, “maybe after all we will get to a more global framework on privacy matters.”

**Take Precautions**

LaFrance said that under the GDPR, “the burden will be on the data controller to demonstrate that the processing of high risk data can be carried out in a way that appropriately limits the risk.”

Companies will need to go through a three-step process—they must decide whether a DPIA is needed for a processing operation; consult with their supervisory authority if a DPIA identifies a high risk; and put in place risk mitigation measures.

The GDPR specifies that DPIAs will be required for any processing to analyze personal data that is “based on automated processing, including profiling,” and that results in decisions being made about data subjects.

Companies might opt for a precautionary approach to carrying out DPIAs. “The key message is: if in doubt, do one,” James said. He added that DPAs must be consulted if a DPIA identifies “a high level of unmitigated risk.”

LaFrance said it was “unclear how supervisory authorities will cope with what could be a very high volume of consultations in an efficient and effective manner.”

The GDPR states that when a data controller consults with a DPA over high-risk processing, and the DPA considers “the controller has insufficiently identified or mitigated the risk,” the DPA has eight weeks to issue advice to the controller, with additional six weeks allowed in particularly complex cases.

Hildebrand said that for small, high-tech companies developing new services or applications based on personal data, this “could be an eternity.”

In addition, the GDPR contains “no provision for confidentiality of the submission” to a DPA in a case of prior consultation over high-risk processing, Hildebrand said.

For companies wanting to safeguard their intellectual property, “that would be one major concern and that could be a disincentive to seek prior consultation,” Hildebrand added.

**Member State Differences**

The final text of the GDPR also embodies the possibility that what is considered high risk in one of the EU’s 28 member countries might not be considered high risk in another.

To guide companies on processing that is likely to be high risk, the GDPR requires national DPAs to issue lists “of the kind of processing operations which are subject to the requirement” to carry out a DPIA.

Tomasz Koryzma, a partner with CMS Cameron McKenna LLP in Warsaw, said he is hopeful that the European Data Protection Board, which will replace the Art. 29 Party, will “help to somehow unify” the definitions.

In case companies might be tempted to seek approval of their data processing from DPAs with less prescriptive lists of high risk processing, they should consider that doing so would “not exclude any liability,” Koryzma said.
More Rigorous Data Management

The GDPR provisions on high risk processing should push companies towards more rigorous management of the personal data that they hold.

“At board level, there is not that much information on how data is actually handled, but this will dramatically change,” Koryzma said.

“The point for the data controller is let's get prepared and audit operations and see what they are processing,” he added.

Controllers will need to look at their relationships with data processors. When controllers issue contracts, there will “now be quite a lot of detailed questions about how processors manage the data,” Koryzma said.

Erik Luysterborg, privacy and data protection leader with Deloitte Enterprise Risk Services in Brussels, said “I don’t think many companies yet have a specific privacy impact assessment process embedded.” They would need to put such a process in place “and then can consider 'when do I use it?'”

Many companies “are in one form or another profiling,” including in their management of employee and customer data, in which case they would be considered under the GDPR to be carrying out high-risk processing, Luysterborg said.

The general thrust of the GDPR was that “you will have to do privacy impact assessments as a rule,” he said.

To contact the reporter on this story: Stephen Gardner in Brussels at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com
Global Perspectives: EU Regulation Binding Corporate Rules Under the GDPR—What Will Change?

EU-U.S. Data Transfers

Binding Corporate Rules offer a solid and comprehensive solution for global data transfers, but the approval process for BCRs will change with the new General Data Protection Regulation. The GDPR will also provide a solid ground for a bright future of BCRs due to their explicit recognition, the author writes.

By Anna Pateraki

Anna Pateraki is senior associate for Hunton & Williams LLP in Brussels.

Binding Corporate Rules (BCRs) are a compliance mechanism with growing importance for global data transfers. They are internal corporate rules, such as codes of conduct, that govern intragroup data practices in a binding and consistent manner worldwide. BCRs demonstrate accountability and build data protection and security into a company's DNA. Within the constantly changing landscape of international data transfers (triggered by the Snowden revelations in 2013 and culminated in the invalidation of Safe Harbor on Oct. 6, 2015, followed by the announcement of the draft Privacy Shield in February 2016), BCRs offer a solid and comprehensive solution for global data transfers. With currently 80 companies having BCRs in place, the number of BCRs is expected to continue to increase.  

1 See press release of the European Commission of Feb. 29, 2016, “European Commission presents EU-U.S. Privacy Shield.”

2 At the time this article was being finalized, 80 companies had BCRs in place, 15 of which were approved within the last 12 months. See European Commission, List of companies for which the EU BCR cooperation procedure is closed.

The adoption of the EU General Data Protection Regulation (GDPR) will change the approval process of BCRs, which will involve the “consistency mechanism” and Commission implementing acts. However, the new process will have a number of benefits for companies and is expected to be streamlined in the future with a view to speeding up the process of BCRs approvals.  

3 For a detailed analysis of the substance of BCRs and the currently applicable approval process, see “Why Do We Need Binding Corporate Rules—A Look to the Future,” BNA Privacy & Security Law Report, March 2, 2015 (43 PRA, 3/5/15).

I. Update on the GDPR

1. Status of the GDPR

On Dec. 15, 2015, the European Parliament and the Council of the European Union (Council) reached political agreement on the upcoming GDPR, which is expected to be officially adopted in the first half of 2016. Currently, the text is being finalized from a legal and linguistic perspective by the EU’s legal services who perform technical adjustments to the text. While minor changes to the text remain possible until all procedural steps have been finalized, these are not expected to have significant
impact on the core elements of the GDPR. Therefore, the version of the text discussed in this article (version of Jan. 28, 2016) is considered to be very close to final. 4

4 See text of the GDPR, version of January 28, 2016, Political Agreement.

In terms of next steps, both the Council and the Parliament will need to adopt the GDPR separately. The Council is expected to adopt the GDPR during the next Justice and Home Affairs (LIBE) Council meeting, which will take place on April 21, 2016. After that, the Parliament will have to receive a recommendation from the LIBE Committee and then adopt the GDPR in a plenary vote, expected for May–June 2016. In the same plenary session, the GDPR will be finalized with the signatures of the presidents and secretaries-general of both the Council and the Parliament, followed by publication in the Official Journal of the European Union (EU) within a few days from signing. The GDPR will take effect 20 days after publication in the Official Journal and will become applicable two years after that date (Article 91).

2. Two-Year Transition Period

The GDPR provides for a two-year transition period until it will apply directly in all EU Member States, thus replacing the various national data protection laws. Companies should use this time to adapt their data practices to the new framework and rethink their compliance model, as the stricter regime of the GDPR is expected to reduce the risk appetite. The transition period will also be useful for data protection authorities (DPAs) who will need to restructure their enforcement and cooperation practices, as well as to secure the necessary resources to be able to exercise the additional powers conferred on them by the GDPR. For example, the Article 29 Working Party has announced that it will start working on the development of the IT systems, human resources and budget for the new tasks of the European Data Protection Board (EDPB) that will be its successor. 5


During the two-year transition period, BCRs will continue to be subject to the same process used today, pending potential further guidance from the Article 29 Working Party. 6 This includes the review of a company's BCRs by the lead DPA, followed by the review of two subsequent co-reviewer DPAs, the confirmation of the reviewed BCRs by the mutual recognition procedure or cooperation procedure, and finally the issuance of national DPA transfer authorizations, where needed. 7

6 See Article 29 Working Party, Work Program of Article 29 Working Party 2016-2018 stating that the transfers subgroup will analyze the impact of the GDPR on existing transfer tools and the existing DPA cooperation procedure.

7 See European Commission, current BCR procedure.

II. Explicit Recognition of BCRs Under the GDPR

1. BCRs as Appropriate Safeguards

Currently, BCRs are not enshrined in law but are established through the standard practice of DPAs and the guidance of the Article 29 Working Party. Once the GDPR takes effect, BCRs will be explicitly recognized as a mechanism "adducing appropriate safeguards" to the transfers of personal data outside the EU (Article 42 (2)). Importantly, the explicit recognition of BCRs covers both BCRs for controllers 8 and BCRs for processors 9 (Article 4 (17)). In addition, BCRs will be available not only to a corporate group but also to a "group of enterprises engaged in a joint economic activity" (Recital 85), which may be interpreted to include business partners.

8 See Article 29 Working Party, the table of Article 29 Working Party on the elements of BCRs for controllers (WP153).

9 See Article 29 Working Party, the table of Article 29 Working Party on the elements of BCRs for processors (WP195).

In the context of examining the validity of the draft EU-U.S. Privacy Shield, the Article 29 Working Party has announced it will also examine the validity of data transfers to the U.S. under the BCRs. 10 In any event, potential upcoming statements or updates to the existing BCRs guidance are not expected to impact the essence of the recognition of BCRs under the GDPR.


2. Minimum Content of BCRs Under the GDPR

As under the current regime, BCRs under the GDPR must include a mechanism to make the BCRs legally binding on the relevant group entities, as well as a mechanism to grant enforceable rights to individuals (Article 43 (1)).
The minimum content of Binding Corporate Rules enshrined in the General Data Protection Regulation is lessened compared to the more exhaustive requirements currently tabled in the guidance of the Article 29 Working Party.

The minimum content of BCRs enshrined in the GDPR is lessened compared to the more exhaustive requirements currently tabled in the guidance of the Article 29 Working Party. Although the core requirements between those two sources are similar in essence, there are some differences including:

- **Principles.** Under the GDPR, BCRs must contain an obligation for companies to describe how they comply with some additional data protection principles, such as the principle of data minimization, privacy by design and by default, and an obligation to define limited storage periods (Article 43 (2)(d)).

- **Profiling.** Under the GDPR, BCRs will have to explicitly give individuals the right not to be subject to profiling (Article 43 (2)(e)).

- **Choice of court.** Under the GDPR, BCRs should give individuals the right to go to court in their country of residence, for example to claim compensation for breach of the BCRs (Article 43 (2)(e) and Article 75). Companies usually want to negotiate the choice of jurisdiction with their lead DPA, to limit legal proceedings to locations where they have facilities to support litigation. The current regime provides this flexibility and BCRs typically provide that individuals can go to court in the country where the company is headquartered in the EU. However, under the GDPR individuals always will have the right to go to their court of residence (Article 75), which may impact the choice of court negotiations. ¹¹

- **Audit.** Similar to the current regime, the GDPR provides that the results of the audit should be communicated to the company’s data protection officer or other person responsible for monitoring compliance with the BCRs, as well as to the board of the company, and should be available to the competent DPA upon request (Article 43 (2)(i)). However, the BCRs for processors per the Article 29 Working Party currently contain much more detail regarding audits. For example, the audit results of the processor should be made available to the controller or the DPA of the controller upon request, and the controller can request that the processor's subprocessors also be audited. ¹²

- **Reporting conflicting legal requirements.** Currently, BCRs for processors include reporting requirements about existing or future legislation applicable to the company that may prevent its fulfilling its obligations under the BCRs. ¹³ Those reporting requirements should be exercised toward the controller or even the DPA of the controller, which is another point for negotiation with the lead DPA. Fortunately for companies, the GDPR seems to limit this otherwise burdensome reporting obligation to be only to the lead DPA.

---


¹² Id., see rules on audits.

¹³ Id., see rules on mandatory requirements of national legislation.

It remains to be seen how the interplay between the various sources of BCRs requirements will affect the way companies draft or negotiate their BCRs with DPAs. In practice, a company considering BCRs will need to look into the requirements spelled out in various legal sources: (1) the minimum content of BCRs under the GDPR (Article 43); (2) the more elaborate BCRs guidance of the Article 29 Working Party, including upcoming guidance from the EDPB, which will continue to issue guidance on the Regulation (Article 66 (1)(b)); and (3) other procedural specifications that may be introduced by the European Commission via implementing acts (Article 43 (4)).
III. The BCRs Process Under the GDPR

1. BCRs Approval & the Consistency Mechanism

The most significant procedural change under the GDPR is that the BCRs approval process will trigger the “consistency mechanism” (Article 43 (1) and Article 57). The consistency mechanism is a new concept introduced by the GDPR that enhances and formalizes the cooperation of DPAs through their participation in the EDPB. Today, the European DPAs have developed specific mechanisms to cooperate in the context of approving BCRs (i.e., mutual recognition procedure, cooperation procedure).

Under the consistency mechanism, DPA cooperation will include more detailed processes, including deadlines, that typically do not apply today. Although today BCRs follow a unique and very specialized approval process, under the GDPR, BCRs will be approved under the same process as other issues (such as those relating to privacy impact assessments, codes of conduct, certification bodies or contractual clauses for data transfers).

Some of the main elements of the consistency mechanism in the context of BCRs include:

• **Lead DPA.** Similar to the current regime, under the GDPR a company will have to identify the “competent DPA” to initiate the process (Article 58 (1)). Where the applicant company has more than one establishment in the EU, the competent DPA will be the lead DPA, meaning the DPA of the “main establishment” of the company in the EU (Article 51a). However, the GDPR contains detailed provisions about the identification of the main establishment (Article 4 (13)) and the cooperation with other “concerned” DPAs (Article 54a), which companies would need to have investigated before starting their BCR efforts. For example, if there is disagreement between DPAs about which DPA should act as the lead DPA, the issue may be escalated to the EDPB for a binding decision (Article 58a (b)) following specific processes and timelines, thus adding on complexity.

• **Draft decision of lead DPA.** The lead DPA will have to review a company's BCRs and communicate a draft decision to the EDPB before approving the BCRs.

• **Opinion of the EDPB.** The EDPB will be composed of representatives of the 28 EU DPAs and of the European Data Protection Supervisor. The opinion of the EDPB on BCRs should be adopted by simple majority within eight weeks, which can be extended by another six weeks (Article 58 (3)).

• **Decision of the lead DPA.** Once the EDPB adopts its opinion, the lead DPA can adopt a decision to approve the BCRs by taking “utmost account” of the opinion of the EDPB, although the opinion is not legally binding. The lead DPA has two weeks in which to inform the EDPB whether it intends to follow the opinion of the EDPB (Article 58 (8)).

• **Dispute resolution.** If the lead DPA informs the EDPB that it does not intend to follow the opinion of the EDPB regarding the BCRs (e.g., content of BCRs), then any DPA concerned may trigger the dispute resolution mechanism by which the EDPB adopts a binding decision (Article 58 (9) and Article 58 (1)(d)). The GDPR gives to the EDPB legal personality and makes it a body of the EU especially so it can adopt legally binding decisions (Article 64 (1)), which is not the case under the current regime. The dispute resolution mechanism is subject to specific processes and timelines, but it is not expected to be used significantly in the context of BCRs, since DPAs are expected to leverage their existing experience of cooperation in the context of BCRs, to avoid disagreements.

The consistency mechanism is intended to cover a variety of multijurisdictional issues under the GDPR. However, at this stage, it is difficult to understand how it will work in the context of BCRs, given the numerous procedures and short timeframes. Also, it is unclear if the consistency mechanism would give all 28 EU DPAs the right to comment on a company's BCRs documents or if this can somehow be avoided by improving the process in the implementation phase, to achieve a regime similar to today's mutual recognition procedure. Given those uncertainties, the GDPR should have scoped down which parts of the consistency mechanism would apply to BCRs, instead of making a general reference to the whole consistency section, which seems to unnecessarily add on complexity.
2. Implementing Acts

Implementing acts are acts of the European Commission setting out uniform conditions for the implementation of legally binding legislation in all EU Member States (Article 291 TFEU). The rules and general principles for the adoption of implementing acts are set out in Regulation 182/2011. 16 The Commission implementing acts aim at executing preexisting European legislation and they do not create new law. 17

16 Regulation 182/2011.
17 This is different from the delegated acts mentioned in the GDPR, which are a law-making procedure with veto rights of the European Parliament and/or Council (Article 290 TFEU).

Under the GDPR, the European Commission can adopt implementing acts to specify the format and the procedures for the exchange of information between controllers, processors and DPAs in the context of the BCRs approval process (Article 43 (4)). Before adopting such implementing acts on BCRs, the Commission will consult with the EDPB (Article 66 (1)(aa)). Currently, the Commission has no executive powers in the context of BCRs, although it participates in the work of the Article 29 Working Party as secretariat. However, under the GDPR the European Commission could play an important role in determining the logistics and processes of BCRs approvals.

The main elements of adopting Commission implementing acts under Regulation 182/2011 are 18:

- **Comitology.** Before adopting an implementing act, the European Commission needs to consult with a committee consisting of Member State representatives and chaired by a Commission official (comitology). The process involves the Council and the Parliament, which can exercise scrutiny, however without having veto rights. As the implementation of the law is the responsibility of the Member States, the Commission cannot adopt a legislative act by itself.

- **Examination procedure.** The GDPR specifies that the Commission can adopt legislative acts on BCRs following the examination procedure (Articles 43 (4) and 87 (2)). The examination procedure is a comitology process (Article 5 of Regulation 182/2011) according to which the Commission submits a proposal to the committee of Member State representatives and the committee needs to deliver an opinion by qualified majority. 19 Simply put, the act is adopted if the committee delivers a positive opinion. If the committee delivers a negative opinion, the act cannot be adopted and the Commission can either submit an amended proposal or refer to an appeal committee, which can decide whether to accept the proposal.

19 Article 5, Regulation 182/2011 on the implementing powers of the Commission. Qualified majority in the Council means at least 55 percent of the members of the Council, comprising at least 15 of them and representing Member States comprising at least 65 percent of the population of the EU (Article 16(4) of the Treaty on European Union).

Depending on the outcome of the various stages, including their respective timelines, it can become complex for the Commission to adopt an implementing act. It remains to be seen what BCRs issues will be regulated via implementing acts and whether any new processes will be introduced that would differ from existing practices.

IV. Benefits of the BCRs Process Under the GDPR

Although the consistency mechanism might sound complicated in its whole, it is not expected that DPAs will make full use of it (e.g., dispute resolution) in the context of BCRs for three reasons: (1) the spirit of the GDPR was to simplify and speed up the BCRs approval process in the first place; (2) the GDPR empowers the Commission to adopt implementing acts that are...
expected to simplify and facilitate the BCRs format and procedures; and (3) the GDPR empowers the EDPB to advise the Commission on BCRs format and procedures, therefore involving national DPAs already at the genesis of those procedures, which can help eliminate disagreements and create a simpler DPA review process (as today with the mutual recognition procedure).

Therefore, the new BCRs process under the GDPR will have a number of benefits to offer, such as:

• **Dealing with one DPA.** Under the GDPR, a company will need to coordinate with one DPA for its BCRs, compared to the currently applicable system of one lead DPA and two co-reviewer DPAs. Also, under the current regime, companies may need to reach out to the various DPAs that do not participate in the mutual recognition procedure and potentially organize meetings with them to close their BCRs approval process. Under the GDPR, the co-reviewer process will no longer be the case, since the consistency mechanism ensures the opinion of all DPAs (hopefully with some simplification in the review process to be specified at a later stage). Dealing with one DPA is very positive for companies, as they can build relationships and trust with their DPA before starting a BCRs project.

• **Abolition of national DPA authorization for data transfers under BCRs.** Under the current regime, companies having their BCRs approved in all relevant countries (via mutual recognition or cooperation procedure) still need to obtain national DPA authorizations in some countries to allow for the transfer of personal data under the BCRs. Since the GDPR does not contain DPA notification and authorization requirements for data transfers, the national authorizations of BCRs will be abolished, where they exist, thus providing a more flexible mechanism in which approval of BCRs and commencement of transfers under the approved BCRs can be merged to occur at the same time. The GDPR does not contain a sunset clause for BCRs approved under the current regime. Therefore, existing national authorizations for data transfers under BCRs will continue to be valid until amended, replaced or repealed by the relevant DPA (Article 42 (5b)).

• **Procedural flexibility.** The GDPR does not exclusively regulate the BCRs process, but gives leeway to the Commission, upon consultation with the EDPB, to create procedural rules in the future as needed to better facilitate the approval process, therefore providing valuable flexibility for companies, similarly to how it is done today with the opinions of the Article 29 Working Party on BCRs.

• **Harmonization.** Today, DPAs in some EU countries do not recognize BCRs (e.g., Portugal), but the explicit recognition of BCRs will help harmonize those inconsistencies due to the direct applicability of the GDPR in all EU Member States.

---

V. Conclusion

BCRs are the future of data transfers and will continue to increase in number. Within the constantly changing environment of data transfers, BCRs provide for a pragmatic method of integrating data protection into the DNA of a company and demonstrating accountability. Even if some changes may be introduced to BCRs in light of the general discussion of regulators on data transfers, the GDPR provides a solid ground for a bright future of BCRs due to their explicit recognition. Although the consistency mechanism that will apply to the approval of BCRs currently seems complex, the overall process is expected to be simplified at a later stage by Commission implementing acts and the guidance of the EDPB, to essentially speed up the BCRs approval process for companies.

---

20 Article 29 Working Party, National filing requirements for controller BCR (BCR-C).
Privacy Law Watch™
August 29, 2016

Data Transfers

The EU-U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options

EU-U.S. Privacy Shield

Baker & McKenzie attorneys discuss the pros and cons of the recently-approved EU-U.S. Privacy Shield and compare it to other options available for cross-border data transfers from the European Economic Area to the U.S. When companies choose an appropriate compliance mechanism to establish adequate safeguards for data importers and onward transferees outside the EEA, they should carefully analyze their particular situation, the authors write.

By Lothar Determann, Brian Hengesbaugh and Michaela Weigl

Lothar Determann is a partner in Baker & McKenzie LLP’s Palo Alto office and is a member of the firm's Global Privacy & Information Management Working Group. He also teaches data privacy and e-commerce law at the University of California Berkeley School of Law, Hastings College of the Law and the Freie Universität Berlin.

Brian Hengesbaugh is a partner in Baker & McKenzie LLP's Chicago office and serves as chair of the firm's Global IT/C Data Security Working Group. Prior to joining the firm, Mr. Hengesbaugh earned a Medal Award from the U.S. Department of Commerce for his participation in the U.S.-EU Safe Harbor Negotiating Group.

Michaela Weigl is an associate at Baker & McKenzie's Frankfurt office and practices data protection and information technology law.

This article reflects the authors’ personal opinions and not those of Baker & McKenzie, its clients or others.

Since Aug. 1, 2016, companies in the U.S. can join the EU-U.S. Privacy Shield Program operated by the U.S. Department of Commerce (European Commission Decision 2016/1250 of July 12, 2016) (134 PRA, 7/13/16). More than 70 companies joined almost immediately (158 PRA, 8/16/16). Others are considering if and when they should join and what alternatives they have.

I. How Can U.S. Companies Join the Privacy Shield?

U.S. companies can certify online to Commerce that they comply with the Privacy Shield Principles after they conduct and
document a self-assessment. Commerce reviews the applicants' submission information and privacy policy and can also request information regarding onward transfer agreements. See, Privacy Shield Adequacy Decision, L 207/51, Accountability For Onward Transfer, 3.a.(vi).

II. Why Should U.S. Companies Join the Privacy Shield?

U.S. companies consider joining Privacy Shield for ease of doing business with European companies and customers.

Companies established or using equipment in the European Economic Area (EEA)—the 28 EU member states plus Iceland, Liechtenstein and Norway—are prohibited from sharing personal data with affiliates, vendors, customers and anyone else outside the EEA, unless an adequate level of data protection in the recipient jurisdiction is assured or an exception or derogation applies. This prohibition stems from the EU Data Protection Directive of 1995 (95/46/EC) (EU Data Protection Directive) and a comparable requirement will continue to apply when the new General Data Protection Regulation (GDPR) becomes effective on May 25, 2018 (see Art. 25 of the EU Data Protection Directive and Art. 44 of the GDPR). In the Directive and in Art. 4 No. 1 GDPR, the term “personal data” is broadly defined to include any information relating to an identifiable individual. Art. 4 No. 1 GDPR defines “personal data” as follows:

... “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Practically, companies cannot conduct any business without sharing at least some contact information and many transactions require more intensive information sharing. Therefore, companies in the EEA need to ensure adequate data protection safeguards to do business or otherwise transmit data outside the EEA.

Brian Hengesbaugh and Amy de La Lama, Cross-Border Data Transfers, 520 Privacy & Data Security Practice Portfolio Series (Bloomberg BNA).

Companies in the European Economic Area need to ensure adequate data protection safeguards to do business or otherwise transmit data outside the EEA.

The European Commission has approved a few countries as generally assuring adequate data protection levels, including Argentina, Canada, Israel New Zealand, Switzerland and Uruguay, but has not issued a blanket adequacy finding for all of the U.S., even though U.S. data privacy laws are in many respects more specific, effective and up to date than data protection laws in Europe and other countries. Lothar Determann, Adequacy of data protection in the USA: myths and facts, International Data Privacy Law (forthcoming, 2016); US-Datenschutzrecht—Dichtung und Wahrheit, NvWZ 2016, 561.

In 2000, the European Commission issued a uniquely limited adequacy finding for the U.S. whereby U.S. companies would be deemed to assure adequate data protection if they joined a “Safe Harbor” program that the U.S. Commerce Department had agreed with the European Commission to enable U.S. companies to satisfy EU adequacy requirements. Fifteen years and approximately 4,500 company registrations later, the Court of Justice of the European Union (CJEU) invalidated the Commission's adequacy decision from 2000 on Oct. 6, 2015 due primarily to concerns that the Safe Harbor itself did not embed protections against U.S. law and policy on government surveillance. Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, judgment of Oct. 6, 2015 (194 PRA 194, 10/7/15); L. Determann, U.S. Privacy Safe Harbor—More Myths and Facts, Bloomberg BNA Privacy & Security Law Report, 14 PVLR 2017 (2015) (216 PRA 216, 11/9/15). For now, Commerce continues to maintain the Safe Harbor program, but has already announced that it is no longer accepting new registrations, and will discontinue accepting annual re-certifications for existing Safe Harbor companies as of the end of October 2016.

After the CJEU challenge to the Safe Harbor program, the European Commission and Commerce intensified their work on a successor program, which they had been working on for a couple of years already. Brian Hengesbaugh, Amy de La Lama, Michael Egan, European Commission Reaffirms Safe Harbor and Identifies 13 Recommendations to Strengthen the Arrangement, Bloomberg BNA Privacy & Security Law Report, 12 PVLR 2013 (2013) (242 PRA, 12/17/13). They created the EU-U.S. Privacy Shield program to address all concerns that the CJEU had raised. On July 12, 2016, after obtaining all requisite approvals and engaging in appropriate consultations, the European Commission issued its decision finding that “the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the EU-U.S. Privacy Shield.” Article 1.1 of the Privacy Shield Adequacy Decision, L 207/35. See also Gilbert/van
Lothar Determann, Brian Hengesbaugh, Michaela Weigl, Baker & McKenzie LLP, The EU-U.S. Privacy Shield Versus Other EU

about Privacy Shield in the context of the annual review of the program, and that the EU data protection authorities will not

collectively, the Article 29 Working Party of EU Data Protection Authorities affirmed that Privacy Shield offers “major

improvements” as compared to Safe Harbor, and has issued statements indicating that it will raise any ongoing concerns

about Privacy Shield in the context of the annual review of the program, and that the EU data protection authorities will not

plan to challenge the program collectively for at least a year.

III. What Other Hurdles to International Data Transfers Apply in the EEA?

Companies in the EEA have to overcome three hurdles before they can lawfully transfer personal data to a company in the

U.S.: (1) generally applicable local compliance obligations, (2) general prohibitions on data processing, including data

disclosures to third parties (whether domestic or international), and (3) prohibitions on international data transfers outside

the EEA. Any violation at either level will cause the data transfer to be ultimately unlawful. See non-binding guidance of March 19,

2009 from European Commission Data Protection Unit—Frequently Asked Questions relating to Transfers of personal data

from the EU/EEA to Third Countries, p. 18.

1. First Hurdle: Local Compliance. Companies in the EEA have to comply with a number of formal and substantive data protection law requirements. For a country-by-country overview, see Baker & McKenzie Global Privacy Handbook (2016 Edition) and Determann's Field Guide to Data Privacy Law, 2nd Ed. (2015). Please also see Determann/Kramer/Stoker/Weigl, Going Global Online, Basic E-Commerce and Data Privacy Considerations, Bloomberg BNA Privacy and Security Law Report, Jan. 12, 2015, p. 6 seq. (10 PRA, 1/15/15). These requirements apply regardless of whether data is transferred or not.

Data controllers have to notify data subjects about all relevant details of data processing, including the legal basis for the collection, use and other processing of personal data (see Art. 13 and 14 GDPR), as automated data processing is by default prohibited in the EEA. See Michaela Weigl, The EU General Data Protection Regulation's Impact on Website Operators and eCommerce, Comp. Law Rev. Int'l, August 2016, p. 102-108. Companies can justify data collection with consent from the data subject, a need to perform contractual obligations, statutory requirements to collect data, legitimate interests and a number of other reasons (see Art. 6 GDPR).

Some EEA member states also require that companies notify national data protection authorities or appoint data protection officers. Lothar Determann and Denise Lebeau-Marianna, Getting a Grip on International Data Protection Authority Filings, 10 BNA Privacy & Security Law Report 639 (2011) (193 PRA, 10/5/11); Lothar Determann and Christoph Rittweger, German Data Protection Officers and Global Privacy Chiefs, BNA Privacy & Security Law Report (2011) . Under the GDPR, more companies will have to appoint data protection officers throughout the EEA and notification requirements may be reduced or abolished (Art. 37 and recital 89 of the GDPR respectively).

2. The Second Hurdle: Disclosures. Even if a company is perfectly in compliance with local data privacy laws (first hurdle) and it also meets the specific requirements for transfers outside the EEA (third hurdle, discussed next), it is not a given that such a company may disclose a particular item of personal data at all to another data controller. Even a wholly-owned, closely-held subsidiary that discloses personal data to its parent company in the same or in another EEA member state has to justify the disclosure. Thus, as a second hurdle to international data transfers, the company in the EEA has to make a case for why the disclosure is permitted despite the general prohibition on processing. This second hurdle is often overlooked by companies focusing on the first and third hurdle.

As with respect to any other processing, companies can theoretically justify disclosures by obtaining valid consent or demonstrating a necessity to transfer data in order to perform a contract with the data subject or comply with local laws. But, data subjects tend to be reluctant to agree to data disclosures and contractual necessities are often not clearly present to justify transfers. For example, an employer needs to collect and process certain personal data to pay its employees, monitor and reward their performance, provide benefits coverage and report and withhold taxes, in accordance with contractual and statutory obligations as an employer. But, it is less clear whether the employer may also disclose employee information to its ultimate parent company, which is a common practice in many multinational groups.

Bloomberg Law

© 2016 The Bureau of National Affairs, Inc. All Rights Reserved. Terms of Service

// PAGE 3
Many multinationals may be able to refer to legitimate interests in this respect (see Art. 6 (f) GDPR, recital 48 GDPR); specifically, small subsidiaries without human resources department may be able to demonstrate legitimate interests or even a contractual necessity for transfers to a 100 percent parent company that manages payroll and other human resources functions for its smaller subsidiaries. But, a larger subsidiary with stand-alone administrative functions may find it more difficult to justify disclosures, because some of the functions and data could also be kept locally.

There are good arguments that multinational businesses will succeed in showing needs for human resources disclosures regarding some data categories that the U.S. parent company legitimately needs, e.g., for cross-border projects and career management, secondments and employee stock option grants. Also, subsidiaries in the EEA that act as sales representatives for U.S. parent companies should be permitted to disclose customer contact information based on legitimate interests for purposes of enabling the U.S. parent company to conclude and perform sales contracts with customers in the EEA. Similarly, companies may have to share certain customer data with logistics providers (to deliver products) and manufacturers (to support expeditious recalls or warranty support). But, independent resellers, for example, may find it more difficult to justify disclosures of consumer data to unaffiliated suppliers.

Where companies cannot otherwise justify data disclosures, they can also consider an engagement of the recipient company as a mere data processor under an appropriate data processing agreement. Companies do not have to further justify data disclosures to service providers if they concluded a data processing agreement that complies with Art. 28 GDPR. There are good arguments that Art. 28 GDPR constitutes a statutory permission for the processing if requirements are complied with, see Niko Härting, May 10, 2016 CR-online.de Blog; and Lothar Determann, Data Privacy in the Cloud—Myths and facts, 121 Privacy Law & Business 17 (2013); L. Determann, EU Standard Contractual Clauses for Transfers of Personal Data to Processing Service Providers Reassessed, BNA Privacy and Security Law Report 10 PVLR 498 (2011) (61 PRA, 3/30/11).

3. Third Hurdle: Transfers Outside the EEA. Companies have to cross only the two hurdles previously discussed with respect to data disclosures within the EEA or to countries that the European Commission has general declared to assure adequate safeguards, i.e., Argentina, Canada, Israel, New Zealand, Switzerland and Uruguay and others. The same applies with respect to U.S. companies that join the Privacy Shield, based on the adequacy decision of the European Commission of July 12, 2016. But, with respect to any data transfers to other countries outside the EEA or to U.S. companies that do not participate in the Privacy Shield program, companies have to cross a third hurdle, namely the general prohibition on international data transfers.

In this respect, companies in the EEA have a number of different options to make transfers subject to appropriate safeguards or otherwise qualify for derogations or other exceptions (see Articles 44 through 49 of the GDPR), including the following:

- explicit consent from the data subject;
- a need to perform a contract with or in the interest of the data subject;
- important reasons of public interest;
- the establishment, exercise or defense of legal claims;
- vital interests of the data subject or of other persons
- Standard Contractual Clauses; and
- Binding Corporate Rules (and, under the GDPR also approved Codes of Conduct).

IV. What Requirements Do the Alternative Data Transfer Vehicles Present?

All alternatives come with strings attached, including the following:

1. Consent and contracts. Companies can legitimize many types of data processing and transfers by obtaining valid consent from the data subjects, i.e., the persons to whom the data relates, or by undertaking contractual commitments that necessitate the transfer (Art. 49.1 a) and b) GDPR). Valid consent and necessities under contracts can help overcome each of the three hurdles. But, consent is valid only if it is freely given, specific, informed and unambiguous, and it can be revoked at any time.
Lothar Determann, Brian Hengesbaugh, Michaela Weigl, Baker & McKenzie LLP, The EU-U.S. Privacy Shield Versus Other EU

2016, the Privacy Shield Principles weigh in at 19 pages and the adequacy decision at 112 pages. This increase in word
Harbor Principles took up 2.5 pages and the Commission's adequacy decision 40 pages in the Official Journal of the EU; in
At first sight, the Privacy Shield Principles are more elaborate and rigid than the Safe Harbor Program: In 2000, the Safe
V. How Does Privacy Shield Compare to the Predecessor Safe Harbor program?

2. Standard Contractual Clauses. If a company within the EEA agrees with a company outside the EEA that the latter will
comply with Standard Contractual Clauses approved by the European Commission for data transfers to controllers (Controller
SCC 2004) or processors (Processor SCC 2010), then “adequate safeguards” are presumed. Art. 46 para. 2 c) GDPR; Brian
Hengesbaugh, Michael Mensik, Lothar Determann, Global Data Transfers and the European Directive—A Practical Analysis
Determann, EU Standard Contractual Clauses for Transfers Of Personal Data to Processing Service Providers Reassessed,

Currently available Standard Contractual Clauses will be grandfathered under the General Data Protection Regulation unless and until the Commission amends them or the Court of Justice for the European Union invalidates the applicable adequacy decision.

Currently available Standard Contractual Clauses will be grandfathered under the General Data Protection Regulation unless and until the Commission amends them or the Court of Justice for the European Union invalidates the applicable adequacy decision (Art. 46.5 sent. 2 GDPR). In order to enjoy the benefit of the adequacy finding of the European Commission, the parties may not modify the Standard Contractual Clauses in any manner that would contradict, indirectly or directly, the clauses or the data protection rights of the data subjects (recital 109 GDPR). Companies are in principle free to modify the clauses or draft their own agreements from scratch, but such “homemade” agreements are subject to full scrutiny by every EU member state and may trigger various additional requirements to notify or obtain approval from local authorities (which can be time-consuming, costly and difficult to manage). But, companies are generally permitted to add provisions that do not affect the privacy protections in the clauses, such as indemnity rules, without implicating the European Commission's binding decision, as expressly noted in the Standard Contractual Clauses.

2. Standard Contractual Clauses. If a company within the EEA agrees with a company outside the EEA that the latter will
comply with Standard Contractual Clauses approved by the European Commission for data transfers to controllers (Controller
SCC 2004) or processors (Processor SCC 2010), then “adequate safeguards” are presumed. Art. 46 para. 2 c) GDPR; Brian
Hengesbaugh, Michael Mensik, Lothar Determann, Global Data Transfers and the European Directive—A Practical Analysis
Determann, EU Standard Contractual Clauses for Transfers Of Personal Data to Processing Service Providers Reassessed,

3. Binding Corporate Rules. For intra-group data transfers, multinational groups can also submit to Binding Corporate Rules
(BCRs), i.e., binding commitments that reflect and safeguards compliance with EU data protection laws on a group of
companies. Art. 46.2(b) and 47 GDPR. BCRs cannot legitimize data transfers to unaffiliated entities, such as customers,
suppliers, distributors, service providers, civil litigants, government agencies and other entities. Art. 47 para. 2 GDPR sets out
the minimum specifications that have to be included in BCRs, including, for example, the structure and contact details of the
group of companies, the data transfers or set of transfers (including the categories of personal data), the type of processing
and its purposes, the type of data subjects affected and the identification of the third country, etc. Art. 47 para. 1 additionally
provides that BCRs must be legally binding and apply to and are enforced by the group companies and expressly confer
enforceable rights on data subjects with regard to the processing of their personal data. The European Commission may
specify the format and procedures for BCRs. Art. 47 para. 3 GDPR.

4. Approved codes of conducts or certification mechanisms. When the GDPR applies, companies may also become able to
rely on codes of conduct that industry associations develop if approved by data protection authorities and granted general
validity by the European Commission. Also approved certification mechanisms issued by certification bodies or data protection
authorities may provide appropriate safeguards after the GDPR comes into effect (Art. 46.2 e) and f) GDPR in connection with
Art. 40 and 42 GDPR).

5. Other options. A few other options apply and companies can mix and match. No one size fits all. Each option presents
different advantages and disadvantages in particular scenarios. Notably, with some of these options, companies cannot only
address the third hurdle described in part III.3 of this article (international transfer prohibitions), but also the first and second
hurdle described in parts III.1 and 2 respectively, i.e., general compliance obligations and disclosure restrictions. The following
parts V and VI of this article focus on comparisons, advantages and disadvantages of the different options to legitimize data
transfers.

V. How Does Privacy Shield Compare to the Predecessor Safe Harbor program?

At first sight, the Privacy Shield Principles are more elaborate and rigid than the Safe Harbor Program: In 2000, the Safe
Harbor Principles took up 2.5 pages and the Commission's adequacy decision 40 pages in the Official Journal of the EU; in
2016, the Privacy Shield Principles weigh in at 19 pages and the adequacy decision at 112 pages. This increase in word
count parallels the growth of EU data protection legislation from the 1995 EU Data Protection Directive on 19 pages to the
2016 GDPR on 88 pages.
More substantively, the Privacy Shield arrangement contemplates annual reviews and updating of the Privacy Shield Principles as well as a number of strengthened or new privacy safeguards such as requirements regarding more detailed privacy notices (calling out details on liability, access rights and dispute resolution), more robust onward transfer contracts and access to such contracts by the Commerce Department, and data minimization, data retention, independent recourse mechanisms at no cost to the individual, as well as publication requirements relating to non-compliance. Companies that voluntarily leave the program must return or delete all previously received personal data or continue to apply the Privacy Shield Principles to such data and recertify compliance on a perpetual, annual basis. If the Commerce Department removes a company from the Privacy Shield Program, the company must delete or return previously collected data (Section 3 of Annex II).


VI. How Does the Privacy Shield Compare to Other Data Transfer Options?

Companies can assess the available options (see III.3 above) based on various different criteria, including the following dozen:

1. **Substantive compliance obligations.** The Privacy Shield Principles of 2016, the Processor SCC 2010 and the Controller SCC of 2004 were created over a span of 12 years with input from different organizations, including the U.S. Commerce Department and the International Chamber of Commerce. Each compliance vehicle contains substantive terms that are intended to commit U.S. companies to core principles of EU data protection laws, but each document uses different verbiage and nuances, which will affect companies differently depending on their business focus and overall situation. For example, the Privacy Shield Principles are specific regarding opt-out rights to onward transfers, dispute resolution process, and data retention.

   The Processor SCC and Controller SCC contain more generalized descriptions on these issues, although it is expected that these clauses will be updated with more specificity in the coming months to respond to the rigors of GDPR. The specifics of the substantive compliance obligations companies must assume in BCRs will depend on what they can achieve in their negotiations with authorities for approval of their BCRs. With respect to emerging solutions, such as Codes of Conduct, the specifics of the substantive requirements will depend on private sector proposals and views of data protection authorities in the approval processes. Where companies rely on consent or contractual necessities, they define their substantive compliance obligations in the terms they present to the data subjects in contracts and privacy notice forms, although the sufficiency of such terms may be subject to review and approvals of authorities depending on national rules.

2. **Flexibility and configurability.** When companies are able to obtain consent or contractual agreements with data subjects, they may have the great advantage that they can tailor the scope of the consent or contract to their particular situation and avoid having to adapt to the more regulated frameworks of the Standard Contractual Clauses, the BCRs, the EU-U.S. Privacy Shield, Codes of Conduct or certification schemes.

   But, consent is valid only if consent is freely given, specific, informed and unambiguous. For international transfers outside the EEA consent additionally has to be explicit. It is not always practical to meet these requirements. Brian Hengesbaugh, Michael Mensik, and Amy de La Lama, Why Are More Companies Joining the U.S.-EU Safe Harbor Privacy Arrangement, International Association of Privacy Professionals (IAPP) Privacy Advisor (January 2010). Some types of businesses do not have any direct relationship with data subjects and they can therefore not approach the data subjects with a request for consent, e.g., cloud, SaaS or outsourcing service providers and companies that host data or websites to which others submit information that may include personal information on EU residents.
Consent is valid only if consent is freely given, specific, informed and unambiguous. For international transfers outside the EEA consent additionally has to be explicit. It is not always practical to meet these requirements.

Businesses might also have difficulties meeting the “voluntariness” requirement: For example, the data protection authorities in most EEA member states presume that employee consent is coerced, hence involuntary, given the typical imbalance of power in the employment relationship. See, for example, Art. 29 Working Party, WP 193, accessed August 7, 2016; L. Determann and L. Brauer, Employee Monitoring Technologies and Data Privacy—No One-Size-Fits-All Globally, 9 The IAPP Privacy Advisor, 1 (2009); L. Determann, When No Really Means No: Consent Requirements for Workplace Monitoring, 3 World Data Protection Report 22 (2003) (187 PRA, 9/26/03).

Additionally, recital 43 GDPR states that consent should not provide a valid legal ground where there is a “clear imbalance” between the data subject and the controller, not providing examples for “clear imbalance.” The term “clear imbalance” might be interpreted as already interpreted by many data protection authorities in employment relationships, however, it might also be extended to other cases, e.g. if a consumer concludes a contract with a company. In such case relying on consent could become an unreliable solution. Most companies also find it challenging to obtain and maintain consent with sufficient specificity, as technology, business practices and purposes change constantly and force companies to update consent forms frequently. It is worth noting that companies are required to notify data subjects about the company’s data processing practices in any event, whether or not the company relies on consent (see Art. 13, 14 GDPR). Yet, data protection authorities and courts might apply higher standards of scrutiny with respect to the amount of information that is required to render consent informed and explicit, compared to a situation where a particular data processing activity is permissible without consent and notification of data subjects is required in the general interest of transparency. Another important consideration is that data subjects can revoke voluntary consent at any time. Therefore, in practice, companies often cannot—or do not wish to—rely on consent to legitimize international data transfers, at least not as the sole compliance measure.

Similarly, contractual obligations vis-à-vis data subjects are not always in place or suited to justify data transfers. Some companies are able to bolster their position regarding data subject consent by additionally creating contractual obligations that in turn create a necessity to engage in certain transfers. For example, if a company contractually agrees with a data subject to retain certain third parties in other jurisdictions to provide services or information, or ship physical items to the data subject, then the company can justify the data transfers to the third parties, as such transfers are necessary to perform under the contract. Some jurisdictions may apply less stringent requirements to online contract formation as they apply to consent under data protection laws, but many European jurisdictions generally empower courts to scrutinize the fairness of clauses in adhesion contracts beyond the standards applied by U.S. law and jurisprudence. See, L. Determann, Notice, Assent Rules for Contract Changes After Douglas vs. U.S. District Court, 12 BNA Electronic Commerce & Law Report 32 (2007); L. Determann and A. Purves, The Glue that Holds it Together: Enforceability of Arbitration Clauses in Click-Through Agreements and Other Adhesion Contracts, 14 Electronic Commerce & Law Report (2009).

3. Geographic and topical coverage. Companies can use consent and contracts with data subjects with respect to all geographies, so these routes are suited to support uniform approaches across geographies. Uniform topical coverage is more difficult, because consent and contractual undertakings are often not an option in certain scenarios—for example, in the human resources context (where freedom to contract is limited and consent deemed coerced) or due to a lack of direct contact with data subjects or a business context that does not induce data subjects to grant consent or conclude contracts.

Companies can also use data transfer agreements and data processing agreements incorporating the Standard Contractual Clauses to legitimize transfers of EEA data to any other country. But, the Standard Contractual Clauses require a significant amount of detail regarding data processing practices and purposes to be included in Appendices to the data transfer agreements, which causes many companies to prepare specific agreements for specific scenarios and this in turn can result in a multitude of limited transfer agreements as opposed to one comprehensive set of rules for all geographies and topics. However, since under the GDPR companies are obligated to prepare “records of processing activities” which must contain, inter alia, the purposes of the processing, a description of the categories of data subjects and of the categories of personal data, the categories of recipients and identification of third countries in case of international data transfers (Art. 30 GDPR), companies are required to map their data anyway.

BCRs, codes of conduct and certification schemes could theoretically provide a comprehensive set of rules and cover any jurisdiction and all data categories. However, BCRs are for intra-group transfers of personal data, i.e., between affiliated companies only, and not for transfers of personal data to and from business partners, such as suppliers, customers, distributors, etc. (Art. 47.1 GDPR). And, companies may logically be reluctant to implement truly global BCRs, because commitments required with respect to EEA data may not be appropriate or affordable for data from other regions or countries.
Implementing data transfer agreements based on the Standard Contractual Clauses does not typically take companies a lot of time in the intra-group context.

Implementing data transfer agreements based on the Standard Contractual Clauses does not typically take companies a lot of time in the intra-group context, because the content of the contracts is largely prescribed and translations in all major European languages are available (courtesy of the European Commission). But, companies with many subsidiaries or particularly dynamic corporate structures (think: acquisition or spin-off sprees) view the implementation of data transfer agreements as a more significant burden, particularly if local operations are reluctant to execute the agreements. Moreover, getting unaffiliated business partners to sign the forms can be challenging (although, more and more sophisticated companies accept the format and wording of the “official” Standard Contractual Clauses as a necessity).

The EU-U.S. Privacy Shield framework can be used to transfer data of any nature, intra-group and vis-à-vis third parties, but it only addresses data transfers from the EEA to the U.S. (or via the U.S. to third countries). It does not cover transfers from the EEA directly to countries other than the U.S..

4. Implementation process and timing. Consent forms and contractual undertakings are relatively easy to prepare and implement in online click-through scenarios, but offline, negotiation and dealing with concerns or push-back raised by data subjects can take a significant amount of time and efforts.

Implementing data transfer agreements based on the Standard Contractual Clauses does not typically take companies a lot of time in the intra-group context, because the content of the contracts is largely prescribed and translations in all major European languages are available (courtesy of the European Commission). But, companies with many subsidiaries or particularly dynamic corporate structures (think: acquisition or spin-off sprees) view the implementation of data transfer agreements as a more significant burden, particularly if local operations are reluctant to execute the agreements. Moreover, getting unaffiliated business partners to sign the forms can be challenging (although, more and more sophisticated companies accept the format and wording of the “official” Standard Contractual Clauses as a necessity).

The greatest administrative burden under the Data Protection Directive used to be and is currently associated with implementing BCRs. Firstly, companies have to decide on the content of the rules “from scratch”: although there is guidance from authorities, no official templates are available, and the publicly available precedents do not necessarily suit all companies. List of companies for which the BCR cooperation procedure is closed; list with links to some approved BCRs. Moreover, BCRs require approval from data protection authorities in every EEA member state. Currently, 21 countries are part of the mutual recognition procedure: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovakia, Slovenia, Spain and the U.K.

Such mutual recognition procedure is quite burdensome and cost intensive. However, under the GDPR at least the content requirements for BCRs are set-out: BCRs must (i) be legally binding, apply to and be enforced by the group of companies, (ii) expressly confer enforceable rights on data subjects with regard to the processing of their personal data and (iii) fulfill certain specifications outlined in Art. 47.2 GDPR (see Art. 47.1 GDPR). Also, the competent supervisory authority must approve BCRs in accordance with the consistency mechanism, i.e., BCRs will formally be recognized across the EU. The competent authority will be the supervisory authority of the main establishment (Art. 56 GDPR). The supervisory authorities must cooperate with each other through the consistency mechanism (Art. 63 GDPR). It remains to be seen, whether the approval process of BCRs will be less burdensome and time consuming under the GDPR.

By contrast, a registration under the EU-U.S. Privacy Shield framework is relatively easy (online filing only) and most EEA member states did not require companies to seek prior approval with respect to data transfers to U.S. Safe Harbor participants, a privilege they may extend to the EU-U.S. Privacy Shield program as it is also an “adequacy” decision. U.S. companies will want to take sufficient time before they submit to the EU-U.S. Privacy Shield framework, because they should conduct the required self-assessment and prepare the relevant due diligence documentation in order to be prepared to answer any questions from Commerce and/or any enforcement actions by the U.S. Federal Trade Commission (FTC).

Such a self-assessment should be undertaken and documented in the context of any of the compliance options; in fact, the ICC Controller Clauses expressly require due diligence efforts as well. But, companies will have to consider the dynamics and implications of needing a corporate officer to sign a declaration regarding compliance and self-assessment, a possible review process by third party validators or dispute resolution process providers as well as the heightened scrutiny from Commerce and/or the FTC regarding applications to join the EU-U.S. Privacy Shield and onward transfer agreements.

It remains to be seen how the newly introduced possibility to adduce appropriate safeguards to legitimize data transfers through approved Codes of Conduct can be implemented (it requires approval from the data protection authority and a European Commission decision). The same applies to the new certification mechanisms which require approval from the data protection authority or from the certification bodies.

5. Ongoing administration. The EU-U.S. Privacy Shield program requires annual re-certification, but changes in the practical details of data processing do not have to be notified to the U.S. Commerce Department. Certification schemes per Art. 42 of the GDPR will be limited to a maximum period of three years and may be renewed. Other compliance options require actions in case of changes (e.g., additional consent, updating contracts or modifying BCRs), but no annual or routine actions in the absence of changes. Approved Codes of Conduct may or may not require ongoing administration, depending on their
individual rules.

6. Onward transfers. As companies decide on a mechanism to legitimize their data transfers from the EEA, they should look ahead and consider the implications of each compliance option for the data recipient outside the EEA and its ability to share data originating from the EEA with onward transferees, such as external service providers, business partners, government agencies (e.g., in case of investigations, litigation or reporting obligations) and other non-EEA affiliates (e.g., subsidiaries in North or South America or Asia).

   As companies decide on a mechanism to legitimize their data transfers from the European Economic Area, they should look ahead and consider the implications of each compliance option for the data recipient outside the EEA

   a. Onward transfer based on consent. If a U.S. company receives the EEA data based on valid consent or a necessity to perform contractual obligations, the U.S. data importer does not assume any specific obligations, except as the U.S. data importer may commit to in the context of the consent, or otherwise agree contractually with any data exporter in the EEA. In the absence of contractual obligations, the U.S. data importer would not face any direct restrictions under EU data protection law. Of course, particularly in the context of HR data transfers, the U.S. data importer would be indirectly affected by compliance obligations on its EEA-based subsidiaries, the data exporters. The European data exporters should not allow the onward transfers, unless the data subjects have been informed as necessary, and the transfers are covered by the scope of the consent or necessity to perform contractual obligations.

   b. Onward Transfers based on Standard Contractual Clauses. U.S. companies that agree to the Controller SCC 2004 and Processor SCC 2010 must pass on their obligations verbatim to onward transferees. This is fairly easy to achieve in the intra-group context, but can be difficult or impossible with respect to some categories of unaffiliated onward transferees, e.g., in the context of litigation pre-trial discovery, if a foreign government demands access to data in the context of investigations (this will likely not be different under the GDPR), if a foreign regulator or law enforcement authority seeks to compel access or when dealing with business partners that do not otherwise have to or want to submit to EU data protection laws. Brian Hengesbaugh and Michael Mensik, Global Internal Investigations: How To Gather Data and Documents Without Violating Privacy Laws, BNA International World Data Protection Report, Volume 8, Number 7 (July 2008). But, since many internationally active business have become familiar with the workings of EU data protection laws, it seems to become easier and easier to obtain signatures on onward transfer agreements that reference the Standard Contractual Clauses, particularly data processing agreements based on SCC 2010. The Model Controller Contracts tend to be relatively easy to implement with respect to group-internal data transfers and usually do not bring about insurmountable obstacles with respect to onward transfers to unaffiliated entities.

   Under the Model Controller Contract, the data importers outside the EEA are not explicitly obligated to implement any particular mechanisms with respect to onward transfers to data processors. But, for various practical reasons, data importers outside the EEA have to sign onward transfer agreements with data processors anyhow. Firstly, onward data recipients cannot be qualified as mere data processors unless they are contractually obligated to act only on behalf, in the interest and per instructions of a data controller. Secondly, the data importer assumes full responsibility for all actions and omissions of its agents under the Model Controller Contract and therefore, has to pass on compliance obligations and allocate commercial risks contractually to onward transferees.

   c. Onward Transfers under EU-U.S. Privacy Shield. If a U.S. company registers with the EU-U.S. Privacy Shield, then such U.S. company would be primarily obligated to ensure that it provides notice and choice to data subjects prior to transferring data to other data controllers. In order to provide data subjects with “choice”, the U.S. company would have to obtain affirmative consent regarding sensitive data (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual); with respect to other data, an opportunity to opt out would suffice. An exception for intra-group transfers does not exist, so companies may have to offer “choice” also for data transfers to affiliates unless they enter into group-internal data processing arrangements or rely on exceptions under EU data protection laws per Privacy Shield Principle I.5. Privacy Shield Adequacy Decision, L 207/49.

   EU-U.S. Privacy Shield registrants are permitted to transfer data to data processors subject a contract and must (i) transfer personal data only for limited and specified purposes; (ii) ascertain that the data processor is obligated to provide at least the same level of privacy protection as is required by the Privacy Shield Principles; (iii) take reasonable and appropriate steps to ensure that the data processor effectively processes the personal information transferred in a manner consistent with the data controller's obligations under the Principles; (iv) require the data processor to notify the data controller if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles;
(v) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to Commerce upon request (see Annex 2, II, 3 b) of the EU-U.S. Privacy Shield). These requirements are stricter than onward transfer obligations under the Safe Harbor Principles.

d. Onward Transfers under BCRs. If a multinational business implements BCRs, it could cause all non-EEA based entities to submit to the BCRs and thus cover all direct and onward data transfers within the group. But, the BCRs do not cover any data transfers outside the group. Thus, groups with BCRs would still have to implement other compliance mechanisms for any direct or onward data transfers to non-affiliated companies. If a group commits in BCRs that it will require onward transferees to adopt the same BCRs or accept them with respect to specific data transfers, such a requirement may be very difficult to satisfy in practice as vendors and other unaffiliated third parties will be hesitant to review, understand and commit to another organization’s custom BCRs.

e. Onward Transfers under approved codes of conduct or approved certification mechanisms. Approved codes of conduct or approved certification mechanisms, require binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.

7. Submission to foreign law and jurisdiction. The consent and contractual undertaking route do not present companies with any specific restrictions as to choice of law or jurisdiction (but general public policy limitations apply, e.g., with respect to consumers and employees). The Standard Contractual Clauses, on the other hand, require the data recipients to submit to the data protection laws and the jurisdiction of the courts of the EEA member state from where the European company transfers the data and data subjects have a third party beneficiary right to enforce the data transfer agreements in a local court. With respect to BCRs, the data protection authorities in each EEA member state where the BCRs will be implemented may demand similar protections in connection with the approval process. Alternatively or additionally, data subjects could try to enforce the Standard Contractual Clauses and BCRs in U.S. courts.

The EU-U.S. Privacy Shield framework is largely a creation of U.S. law and enforcement will likely occur primarily in the U.S.: Commerce will scrutinize submissions, handle challenges and possibly request information from organization that register. Also, the FTC is the primary enforcement authority for Privacy Shield violations. And, at least in principle, the FTC, State Attorneys General and private plaintiffs can bring actions on unfair competition, misrepresentation and breach of contract theories in connection with any compliance vehicles.

Courts in the U.S. and EEA courts may take jurisdiction based on traditional rules of civil procedure. Also, with respect to HR data, U.S. companies have to submit to the jurisdiction and audits by EEA data protection authorities, even in the context of the EU-U.S. Privacy Shield program (Annex II, 5.d, Role of Data Protection Authorities of the Privacy Shield Adequacy Decision).

8. Enforcement risks. Regarding Standard Contractual Clauses and BCRs, enforcement actions have so far not yet publicized—neither in the U.S. nor the EU. In the relatively few enforcement cases involving data transfers from the EEA to other countries, the European Data Protection Authorities have so far preferred to take action against the data exporter, i.e., the local entity that was fully obligated to comply with local data protection laws anyhow. At the same time, the validity of the Standard Contractual Clauses themselves are currently subject to scrutiny and may be modified by the Commission proactively or struck down in a similar manner as the Commission decision regarding Safe Harbor.

With respect to the U.S. Safe Harbor program, on the other hand, the FTC had brought more than two dozen enforcement actions and companies that participated in the program have also been subject to challenges to the program itself in Europe. Brian Hengesbaugh, Lothar Determann, Amy de La Lama, and Michael Egan, U.S. Federal Trade Commission Is Serious About Enforcement of the U.S.-EU Safe Harbor Framework, Baker & McKenzie LegalBytes Special Edition (February 2014). The U.S. Commerce Department and the FTC have committed to enforcing the Privacy Shield more rigorously than the Safe Harbor Program in the U.S. and challenges to the program itself are expected in Europe. Therefore, and based on experiences with the Safe Harbor program, some U.S. companies are concerned about potentially greater risks of enforcement actions if they join the Privacy Shield than if they rely on other compliance options.

9. Public relations and business benefits. In the early years of the U.S. Safe Harbor Program, U.S. companies advertised their registration on consumer-facing websites, touted their registration status in whitepapers on privacy-compliance,
U.S.-based cloud or processing services providers will likely sign up, because the EU-U.S. Privacy Shield Principles and EU data protection laws generally do not demand materially more in terms of substantive compliance than what are otherwise required in their services agreements.

U.S.-based cloud or processing services providers will also likely not worry much about signing up, because the EU-U.S. Privacy Shield Principles and EU data protection laws generally do not demand materially more in terms of substantive compliance than what are otherwise required in their services agreements. U.S.-based data processing service providers are also expected to agree to data processing agreements based on the Standard Contractual Clauses 2010. Companies that are not pressured by customers to sign up for the EU-U.S. Privacy Shield and do not want to expose their compliance approach to the public eye might decide not to join the Privacy Shield at this time, and implement data transfer and data processing agreements only.

10. Stability. The EU-U.S. Privacy Shield will be reviewed and possibly renegotiated annually by the European Commission and Commerce. SCC are currently challenged. BCR requirements constantly evolve. Requirements for Codes of Conduct and Certifications are still in the process of being developed. Data subjects can revoke their consent to voluntary data processing at any time. Currently, none of the options offer a great degree of stability.

10. International Interoperability and non-EEA Data. Most U.S.-based multinationals are not only dealing with personal data and compliance requirements from the EEA. Increasingly, other jurisdictions are enacting or updating data protection laws and introduce additional or different requirements. A company that registers under the EU-U.S. Privacy Shield would not benefit from such a registration with respect to personal data or requirements from other jurisdictions, given that the program applies only to data from the EEA and only to U.S. companies. But, companies that participate in the Privacy Shield program should be able to leverage their self-assessment documentation and privacy notices. Consent, data transfer and processing agreements, and BCRs can also be leveraged for many other jurisdictions and modified versions of SCC-based data transfer agreements or data processing agreements are also useful internationally.

12. Formalities. The EU-U.S. Privacy Shield requires a formal compliance declaration from an officer of the company in connection with the initial certification and annual recertification. Participating companies are listed on a public website maintained by Commerce, even if and after they withdraw from the program.

For the execution of contracts based on the SCC 2004 and 2010 and any amendments, a signature from authorized company representatives is also required, but these do not have to be corporate officers. Many multinational enterprises work with centralized powers of attorney to facilitate the execution of routine contract amendments, e.g., when addresses of entities change. Companies do not have to publicly disclose their contracts.

Signature, publicity and other formal requirements relating to BCRs, Codes of Conducts and Certification vary from country to country. The European Commission publishes a list of companies that have obtained approvals for BCRs.

Companies that rely on consents or contracts with data subjects do not have to comply with formal signature requirements and are not added to published lists.

VII. Summary

No one size fits all. Each company (and business unit within decentralized organizations) has to assess its own data flows, business needs and risk sensitivities, and this may cause organizations to select different compliance mechanisms for specific countries, business lines, data categories, use cases and other scenarios. With respect to cross-border data transfers from the EEA, multinational businesses must ensure that all three hurdles are taken. When companies choose an appropriate compliance mechanism to establish adequate safeguards for data importers and onward transferees outside the EEA, they should carefully analyze their particular situation, for example, regarding data categories (sensitive or non-sensitive), data flows, processing needs, ability to obtain contractual justifications or consent from data subjects, ability to implement contracts in the entire data transfer chain and implications of a particular compliance mechanism for various other compliance steps and challenges (such as disclosure requests in the context of litigation or government investigations, whistleblower hotlines,
employee monitoring, etc.). None of the available options is superior for all companies and all circumstances. But, companies that assess their particular situation and all applicable PROs and CONs carefully will often identify a clear favorite for particular data streams and business lines.
Concrete Solution, or Are the Sands Still Shifting? European Data Protection Post-Schrems

EU-U.S. Privacy Shield

Official Responses and Brexit

There is no guarantee that the EU-U.S. Privacy Shield data transfer program won’t be subject to further challenge before the European courts, with dissenting voices continuing to criticize the new deal and uncertainty about how Brexit may impact the situation. Companies would be well advised to consider other methods of legitimizing the transfer of personal data from the European Economic Area to the U.S., or where possible, silo data within the EEA so that cross border data transfer issues don’t arise, the authors write.

In the months following Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Schrems) (14 PVLR 1825, 10/12/15), in which the Court of Justice of the European Union (CJEU) invalidated the European Commission’s Safe Harbor Decision (2000/520/EC), issues with respect to the transfer of personal data from the European Economic Area (EEA) to the U.S. have continued to evolve, leaving little certainty for companies engaged in cross border data transfer. Post-Schrems, personal data can no longer be transferred from the EEA to U.S. companies that self-certified to the Safe Harbor regime without such companies providing an alternative mechanism to adequately protect the data on transfer. As has been previously reported, national data protection authorities (DPAs), both within and outside the EEA, urged data controllers who were previously relying on Safe Harbor to reconsider the legal basis for transferring data from Europe to the U.S., with some DPAs suggesting that companies should enter into “Model Contract Clauses” in order to legitimize such data transfers. However, Model Contract Clauses were seen by some as a temporary solution (with certain German DPAs rejecting this option entirely), and it was widely recognized that a longer-term, more concrete solution needed to be reached to the problem of transatlantic data flows. Following crisis talks between the European Commission and U.S. officials, a deal was announced on Feb. 2, 2016—called the EU-U.S. Privacy Shield—as the proposed solution to this problem (15 PVLR 269, 2/8/16).

The Privacy Shield, in a revised form intended to address criticisms of the February text, was adopted by the Commission on July 12; there is, however, no guarantee that it won’t be subject to further challenge before the European courts, with dissenting voices continuing to criticize the new deal. To complicate matters, the Irish DPA recently referred certain questions...
on the adequacy of the Model Contract Clauses to the Irish Courts for further referral to the CJEU. In short, issues with respect to the transfer of personal data outside the EEA don’t appear to be fully settled and the sands, for now, continue to shift.

The EU-U.S. Privacy Shield

On Feb. 29, 2016, the European Commission issued the various texts which form the Privacy Shield, including a series of letters and written commitments from the U.S. Department of Commerce, U.S. Secretary of State, U.S. Secretary of Transportation, U.S. Department of Justice, the Office of the Director of National Intelligence and the Federal Trade Commission.

Like the Safe Harbor regime, the Privacy Shield requires U.S. businesses to sign up to a series of principles, register to be on a compliance list (called the Privacy Shield List), and self-certify that they meet the regime's requirements if they wish to receive personal data from the EEA. The framework will be largely enforced by the U.S. Department of Commerce and the U.S. Federal Trade Commission, as the U.S. government was reluctant to allow this role to be carried out by the EU DPAs themselves. These U.S. authorities will publish a list of companies which have signed up to the Privacy Shield, and those which have been excluded for breaching its terms.

Broadly, the terms of the Privacy Shield impose stronger obligations on U.S. companies to protect the personal data of individuals within the EEA as compared to the Safe Harbor regime. Notably, there are requirements of greater transparency, increased monitoring of compliance and explicit redress mechanisms, including the establishment of an ombudsperson mechanism tasked with handling complaints from individuals. In addition, as a result of concerns voiced by various parties, including the EU’s Article 29 Working Party (a body comprised of representatives from the national DPAs of all Member States) (WP29), the final version of the Privacy Shield includes a number of critical amendments designed to address specific concerns about the initial proposal (as further discussed below).

Responses

On Feb. 29, 2016, the same day as the publication of the texts which form the substance of the Privacy Shield, the European Commission also published a draft “adequacy decision” which states that, following these commitments, the U.S. can be seen as providing an adequate level of protection of personal data—i.e., equivalent to the protections offered by EU law (15 PVLR 462, 3/7/16). However, this did not mark the agreement as a done deal. Both the WP29 and the European Data Protection Supervisor (EDPS) raised objections to the Privacy Shield as then drafted. In Schrems, the Safe Harbor regime was severely criticized by the CJEU for failing to prevent U.S. authorities (such as the National Security Agency) from collecting EU citizens’ data in bulk. Several parties, including the WP29 and the EDPS have separately criticized the Privacy Shield (as it was presented in February) as not adequately remedying this problem. The WP29 and the EDPS explicitly stated that the February draft of the Privacy Shield failed to ensure protection “essentially equivalent” to EU law.

The Article 29 Working Party was concerned specifically that the February draft of the Privacy Shield did not adequately prevent the U.S. authorities from collecting European Union citizens’ personal data indiscriminately and in bulk.

The WP29 issued its Opinion 01/2016 on the Privacy Shield draft adequacy decision on April 13, 2016, in which it stated that certain “key data protection principles as outlined in European law are not reflected in the [Commission’s] draft adequacy decision and the annexes, or have been inadequately substituted by alternative notions” (15 PVLR 825, 4/18/16)

The WP29 was concerned specifically that the February draft of the Privacy Shield did not adequately prevent the U.S. authorities from collecting EU citizens’ personal data indiscriminately and in bulk. The text of the Privacy Shield allowed U.S. authorities to collect such data in bulk for the purposes of “detecting and countering certain activities of foreign powers; counterterrorism; counter-proliferation; cybersecurity; detecting and countering threats to U.S. or allied armed forces; and combating transnational criminal threats, including sanctions evasion”. The WP29 believed that such broad possible derogations to the principles of data privacy “do not exclude massive and indiscriminate collection of personal data originating from the EU.” Such criticisms have been voiced by many, notably including Max Schrems himself, who said that “Basically the U.S. openly confirms that it violates EU fundamental rights in at least six cases….“ The WP29 also made it very clear that “massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society.”
EDPS

As previously reported, the EDPS, Giovanni Buttarelli, published Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision on 30 May 2016 (15 PVLR 1161, 6/6/16). Buttarelli praised the Privacy Shield as a genuine attempt to improve upon the Safe Harbor regime, noted that several improvements were apparent, and acknowledged the involvement of several key U.S. governmental organisations, particularly the Department of State, the Department of Justice, and the Office of the Director of National Intelligence. However, he also made it clear that the Privacy Shield, as drafted in February, would suffer a similar fate to Safe Harbor unless “significant improvements” were made, and that “progress compared to the earlier Safe Harbour Decision is not in itself sufficient. The correct benchmark is not a previously invalidated decision...."

The EDPS echoed the concerns of the WP29 regarding the bulk collection of European citizens' data by U.S. authorities and felt that the February draft of the Privacy Shield would likely be seen as legitimizing such mass collection. Furthermore, the EDPS was critical of the agreement's lack of provisions concerning data retention.

European Parliament

In May, the European Parliament noted that the Privacy Shield contained “substantial improvements” as compared to Safe Harbor, but that it still contained a number of “deficiencies.” According to the European Parliament, U.S. authorities would still have unacceptably broad access to the personal data of EU citizens. It also echoed the criticisms of others regarding the apparent lack of independence of the new ombudsperson, which would not be “vested with adequate powers to effectively exercise and enforce its duty,” and the proposed redress mechanism which was described as overly complex and needed to be more “user-friendly and effective.”

U.K.

On Feb. 11, 2016, the U.K.'s national DPA, the Information Commissioner's Office (ICO) published a blog post stating that “it is too early to say whether the new Shield provides adequate protection for personal data passed from the EU to the USA.” However, the ICO also said that it “will not be seeking to expedite complaints about Safe Harbor while the process to finalise its replacement remains ongoing and businesses await the outcome.”

At the Westminster eForum on April 28, 2016, U.K. Information Commissioner Christopher Graham urged U.S. companies to put pressure on U.S. government officials to answer the “simple, relevant questions” raised of the Privacy Shield by the WP29. “You can be sure that the European Court of Justice would also be asking these questions,” Graham said, clearly referring to the possibility that the highest court in Europe may invalidate the Privacy Shield if it is not convinced that this agreement genuinely secures an “adequate” standard of protection for personal data which is sent to the U.S. from the EEA.

Amendments to the Privacy Shield

In light of such strong concerns over deficiencies contained in the February draft of the Privacy Shield, negotiations were resumed between the EU and the U.S. In June 2016, a revised agreement was reached which remedied many of these concerns. The White House has confirmed in writing that bulk collection of data will be “as targeted and focused” as possible. The Privacy Shield now explicitly contains rules on data retention, so U.S. companies will be required to delete data they hold which becomes redundant for the purpose for which it was collected. Furthermore, in order to address concerns about the impartiality of the new ombudsperson, the U.S. has agreed that this body will be independent from national security services.

Is the Privacy Shield Now Set in Stone?

On 25 June 2016, the European Commission submitted the revised draft of the Privacy Shield adequacy decision to the Article 31 Committee, a group of representatives of the Member States. The Privacy Shield was formally adopted by the Commission on 12 July 2016, and companies will be able to certify with the U.S. Department of Commerce starting 1 August 2016. However whilst it may appear that the sands are beginning to settle, companies should keep developments under close review, as privacy advocates have already suggested that the Privacy Shield may be challenged before the CJEU, notwithstanding the Commission's declaration that the revised and adopted version reflects the court's requirements.

Fines and Enforcement Post-Schrems

In the months following the Schrems decision, most national DPAs have taken a hesitant approach to enforcement against U.S. companies which continue to transfer data from the EEA to the U.S. on the sole basis of Safe Harbor. Indeed, the U.K. ICO stated that it will be “sticking to [its] published enforcement criteria and not taking hurried action whilst there's so much uncertainty around and solutions are still possible.” However, a German DPA took a different view and has fined Unilever PLC, Adobe Systems Inc., and Punica Getranke GmbH (15 PVLR 1227, 6/13/16) (although admittedly fairly small sums) for...
transferring personal data to the U.S. from Europe and relying only on Safe Harbor post-Schrems.

The U.K. would presumably not wish to significantly diverge from the General Data Protection Regulation for fear of being deemed "not adequate" by the European data protection authorities.

Impact of Brexit

On June 23, 2016, the U.K. public voted, by a 52 percent majority, to leave the EU. It is still very unclear whether, and/or on what terms, this will happen. However, assuming the U.K. does in fact leave the EU, the U.K. will no longer be bound by EU data protection law or covered by the Privacy Shield, nor will it be bound by the obligations of the EU General Data Protection Regulation (GDPR) (unless it remains a member of the EEA). There is likely to be a period of cross-over between the coming into force of the GDPR (25 May 2018) and the U.K.’s departure from the EU; although it is uncertain whether the U.K. government will honour its obligations under the GDPR during this period.

The ICO said in an official statement on 19 April 2016 that “the U.K. will continue to need clear and effective data protection laws, whether or not the country remains part of the EU.” Furthermore, if the U.K. leaves the EU, the U.K.’s data protection regime will still need to be recognized by the European Commission as “adequate” (i.e. providing an equivalent standard of protection as is afforded in the EU) in order for personal data to be freely transferred from the EU to the U.K. post-Brexit.

The possible future invalidity of Model Contract Clauses as a means of lawful data transfer to the U.S. may well have influenced the Article 31 Committee’s decision to approve the EU-U.S. Privacy Shield as an alternative.

It seems highly likely that a failure to comply with at least the spirit of the GDPR would be fatal to such an adequacy decision; thus the U.K. would presumably not wish to diverge from the GDPR for fear of being deemed “not adequate” by the European data protection authorities. However, whether the U.K. will retain the provisions of the GDPR verbatim remains to be seen. Indeed, if the data protection laws adopted by the U.K. are not deemed adequate by the European Commission, it is also not out-of-the-question that the Privacy Shield or a similar regime may be put in place between the U.K. and the EU to provide adequacy to personal data on transfer.

Model Contract Clauses Called Into Question

On May 25, 2016, the Irish Data Protection Commissioner stated that it will refer the legality of personal data transfers under the Model Contract Clauses to the Irish High Court for declaratory relief, with the intention of this question being further referred to the CJEU. It has been suggested that the CJEU may hold these clauses invalid for much the same reason as it did for Safe Harbor in Schrems, namely that the Model Contract Clauses fail to prevent the wholesale collection of European citizens’ personal data by U.S. authorities.

As the Privacy Shield has now been approved by the Article 31 Committee and will shortly come into effect, this issue will likely be avoided. Indeed, the possible future invalidity of Model Contract Clauses as a means of lawful data transfer to the U.S. may well have influenced the Article 31 Committee’s decision to approve the Privacy Shield as an alternative; although global companies such as Facebook Inc.—Facebook has been involved in numerous legal battles relating to data protection, including the Schrems case—will likely be following the Irish High Court case, and possible future CJEU referral, carefully.

Conclusion

The months of uncertainty surrounding European data protection and EU-U.S. data flows seem to be slowly settling; though given ongoing criticism of the various methods of cross border data transfer, companies should continue to closely monitor this landscape. This new agreement will allow certified U.S. companies once again to lawfully transfer personal data from the EEA to the U.S. without having to rely on Model Contract Clauses, the legality of which is currently being challenged, or face fines and other enforcement action by the various European DPAs.

As to Brexit, if the U.K. does leave the EU, it will not be legally bound to keep its national laws in conformity with the obligations contained in the GDPR (unless it remains part of the EEA); however it seems highly likely that the U.K. would...
choose to do so, due to the fear of its data protection laws being deemed not to offer “adequate” protection as compared to EU law. The Privacy Shield may offer a concrete solution to cross border data transfer but given ongoing scrutiny, companies would be well advised to also consider other methods of legitimizing the transfer of personal data from the EEA to the U.S., or where possible, silo data within the EEA so that cross border data transfer issues do not arise.
EU Certificate May Be U.S. Data Transfer Alternative

BNA Snapshot

• New EU privacy regulation allows for data protection certification and privacy seal managed by privacy regulators
• Privacy certification may be basis for legal international data transfers
• Privacy certificate may be alternative to potentially vulnerable EU-U.S. Privacy Shield data transfer pact

By Stephen Gardner

Aug. 3 — A European Union-administered privacy trust mark system might provide a viable data transfer alternative to the new but potentially vulnerable EU-U.S. Privacy Shield.

A trust seal program might provide privacy compliance certainty for U.S. companies and their EU associates, help provide a more widespread and effective EU enforcement mechanism and expand the alternatives for legally transferring data to the U.S., privacy attorneys and officials told Bloomberg BNA.

EU privacy regulators said they will release guidance by the end of 2016 on how a trust seal program could work under the new EU General Data Protection Regulation (GDPR).
D. Reed Freeman, a partner and co-chair of the Cybersecurity, Privacy and Communications practice at Wilmer Cutler Pickering Hale and Dorr LLP in Washington told Bloomberg BNA that companies would welcome a wider choice when it comes to mechanisms to legitimize their data transfers.

“There is a vacuum to be filled here. More options in the market is something the market always likes. In general, where compliance certainty can be provided, you'll see widespread adoption,” he said.

Isabelle Falque-Pierrotin, chairwoman of the Article 29 Working Party of privacy officials and president of France's privacy office (CNIL), told Bloomberg BNA that a certification program would help U.S. companies and might even influence privacy leaders in Asia to increase privacy certification efforts.

But some EU privacy officials and attorneys said a trust mark system would be more expensive for U.S. companies to implement than the Privacy Shield.

**Fragile Privacy Shield?**

The Privacy Shield was launched as a replacement for the U.S.-EU Safe Harbor program. The Safe Harbor was invalidated by the European Court of Justice, the EU's top court.

More than 4,000 U.S. companies and tens of thousands of EU companies that relied on the Safe Harbor to legitimize their transfers of the personal data of EU citizens to the U.S. were left with a limited menu of alternatives. Many U.S. companies are expected to join the U.S. Department of Commerce-administered Privacy Shield, but that may only be a temporary fix if the replacement program is itself invalidated by the ECJ.

Commerce opened the doors to the Privacy Shield self-certification scheme Aug. 1.

The Privacy Shield stands on fragile legal ground according to some EU privacy officials, privacy advocacy groups and attorneys, although EU privacy officials recently announced a one-year moratorium on legal challenges to the program.

Another legal alternative, standard contractual clauses (SCCs) may also be in trouble.

SCCs are model contracts established by the European Commission, the EU's executive arm, that companies may adopt in individual business agreements to prove their adherence to principles of the 1995 EU Data Protection Directive (95/46/EC). But the Irish High Court is expected in early 2017 refer SCCs to the ECJ for a ruling on whether they sufficiently protect EU privacy rights.

**EU Privacy Reg Foundation**

The GDPR, which is set to take effect in May 2018, authorizes a privacy certification program overseen by EU privacy regulators.

The GDPR foresees development of codes of conduct and privacy seals, which may be applied broadly for international data transfers.

GDPR Article 42 states that approved codes of conduct and privacy seals that place "binding and enforceable commitments" on data controllers or processors in non-EU countries, and that protect the rights of data subjects, will be recognized as valid for EU data exports.

Carlo Piltz, an information technology and data protection law lawyer with JBB in Berlin, told Bloomberg BNA that privacy certifications under the GDPR would be overseen by privacy regulators or recognized certification bodies and might "be a smooth way to legitimize data transfers."

The EU, however, has limited experience of developing official privacy certification schemes. The predecessor Data Protection Directive authorized development of codes of conduct for EU companies but didn't mention privacy seals.

The GDPR sets up a much more formalized and rigorous architecture for codes of conduct and privacy certification, with privacy regulators playing a central role.
Codes of conduct would be drawn up by industry sectors, or could cover specific types of data processing, and would be validated by the new European Data Protection Board (EDPB) and the European Commission, which would issue a legal act recognizing each code of conduct.

The GDPR also creates obligations for privacy regulators or accreditation bodies to monitor, revoke and record codes of conduct. The EDPB will be the successor body to the Article 29 Working Party of EU privacy officials. Unlike the Art. 29 Party, the EDPB will have some power to resolve disputes among privacy offices from EU countries.

In addition to codes of conduct, certification and data protection seals would be a separate option. Privacy regulators and/or third parties accredited by the regulators would offer certification, which would be valid for a maximum of three years.

**Large-Scale Application**

The overall impact would be greater powers for privacy regulators and the EDPB to legitimize data processing operations, including those carried out in non-EU countries. But the ability to utilize third parties to administer a trust seal system may be the most compelling reason for privacy officials to push for an international data transfer trust seal program.

Falque-Pierrotin said that privacy certification is “a way to ensure compliance efforts on a large scale.”

It is “unrealistic to believe that only the regulators can do the job” of ensuring compliance, and through certification mechanisms, the job would in effect be outsourced, she said. Under the GDPR, privacy offices and the EDPB would be able to recognize certification schemes managed by accreditation bodies.

However, certification “needs to be in an architecture that is defined” by privacy officials and lawmakers, Falque-Pierrotin said. “Certification as an activity needs to be organized. It has to be in a framework,” she added.

The forthcoming Art. 29 guidance on codes of conduct and certification will “clarify how we view this activity of certification,” Falque-Pierrotin said. The guidance will set out parameters on issues such as criteria for certification bodies and what guarantees they should provide to privacy officials, she said.

The EU interest in certification programs may be influential in Asia, where countries are “very much interested in certification,” Falque-Pierrotin said.

**French Certification Experience**

France has been active in its own privacy certification program so stands in a strong position to shepherd any move towards an EU-wide trust mark system.

CNIL is a rarity among EU privacy regulators in that it already issues certification, covering four types of activity:

- privacy audits;
- privacy training;
- data protection and respect for privacy rights in organizational governance; and
- the use of “digital safes” for secure online data storage.
In each of these areas, CNIL issues lists of requirements that organizations must meet to obtain certification and the accompanying trust seal label issued by the privacy office.

Gwendal Le Grand, CNIL director of technology and innovation, told Bloomberg BNA that CNIL’s organizational governance certification may in principle cover international data transfers and would be “recognized as being sufficient in many countries” as a safeguard of data subjects’ rights.

France's experience of certification “will be very useful” in the expansion of certification across the EU, and the CNIL certification for organizational governance “probably can be quickly Europeanized,” Le Grand said.

The certification is grounded in France’s data protection law that transposed the expiring EU Data Protection Directive into national law. That national law will be replaced by the GDPR.

If modified to be in line with the GDPR and recognized by the EDPB, CNIL certification may become available across the EU and could be the basis for a European Data Protection Seal.

“The regulation is drafted in such a way to allow this European seal to emerge,” Le Grand said.

CNIL certification takes up to eight months and is free of charge, though “we don't know yet if the CNIL’s work will continue to be free,” after the transition to the GDPR, Le Grand said.

Trust Marks More Expensive

Another form of certification available in the EU is offered by Bonn, Germany-based EuroPriSe, an independent privacy certification organization spun out of an EU-funded project. EuroPriSe offers a “European Privacy Seal” to information technology products and services, including websites. The seal is valid only in the EU.

Sebastian Meissner, head of EuroPriSe, told Bloomberg BNA certification might replace the Privacy Shield.

However, different transfer mechanisms will co-exist. Obtaining privacy office-approved EU certification may be “a tougher task than to comply with Privacy Shield,” Meissner said. Certification as foreseen under the GDPR would involve “some cost and effort and not all companies are ready to take that road,” he said.

Piltz agreed. He said “the implementation of such seals or certifications might turn out to be costly in terms of time and effort.”

By comparison, the implementation of SCCs “is very easy for companies” and may be done “without much effort,” Piltz added.

To contact the reporter on this story: Stephen Gardner in Brussels at correspondents@bna.com

To contact the editor responsible for this story: Donald G. Aplin at daplin@bna.com
The EU-U.S. Privacy Shield data transfer program will have a substantial impact on how many U.S. companies will be able to receive data from Europe and on how data can be transferred and used, the author writes, noting that although some health-care companies may find the program useful, others may be unable to participate or find compliance too difficult.

By Kirk J. Nahra

Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, specializing in litigation and counselling related to privacy, data security and cybersecurity in the U.S. and across the globe. He chairs the firm’s Privacy Practice and co-chairs its Health Care Practice. He represents companies in virtually every industry in navigating the complexities of privacy and security laws and regulations, across industries and jurisdictions. He can be reached at 202.719.7335 or knahra@wileyrein.com. Follow him on Twitter @kirkjnahrawork.

Health care used to be local. You went to the neighborhood doctor for your physical or to a pediatrician for your kids. If something went wrong, there was a local hospital. You got insurance, if at all, through your employer, who likely went through the local Blue Cross Blue Shield plan. These entities were all independent, and data sharing between these entities was largely limited to sending in claims information so doctors could get paid.

As with most industries, times certainly have changed. Your doctor is part of a large physician group. Your hospital is owned by a national conglomerate. The health insurer may have merged several times. Managed care has made data even more important, and increased movement towards “accountable care” and risk sharing have exploded the need to share data. At the same time, we now have electronic health records, personal health records, health information exchanges, mobile applications, wearables and more, all collecting and sharing our health information, for a broad variety of public and private purposes.

Beyond these developments, health care also is becoming global. The health insurer may have a call center in India. The latest drug is being developed by a company from Europe, using physicians and patients across the globe. Researchers everywhere are developing new health care protocols and exploring the efficacy of new treatments. Your employer is managing health-care costs across its full employee population, which often covers multiple continents.

In the U.S., we are familiar in the health-care industry with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule, which govern the sharing of health information among “covered entities” (doctors, hospitals and other health-care providers and health plans) and their “business associates” (service providers). We also are aware that there are gaps in this structure, driven by the limited scope of the HIPAA rules and the emerging new sources for health-care
We haven't always paid as much attention to the international role in privacy law for the health-care industry. But we need to, as the business of health care is expanding globally and the number of countries with strong privacy rules is growing consistently. There is ambiguity, inconsistency and constant evolution, creating the need for smart, effective privacy officers at health care companies (and companies in virtually all industries).

The latest wrinkle involves the need to find a way to transfer data from one country or region, regulated by one set of laws, to another country, such as the U.S., in a way that complies with all of the applicable laws. For more than a decade, an effective program had been built to transfer individually identifiable data from the European Union to the U.S. Called the “Safe Harbor” program, this self-certification program provided a means for more than 4,000 companies to transfer data to the U.S., across a wide range of industries, including health care.

Recently, in October 2015, the European Court of Justice (ECJ) struck down the Safe Harbor program, driven primarily by concerns about the U.S. government's access to personal data that was transferred under the program (194 PRA 194, 10/7/15). Corporate panic ensued, followed by massive uncertainty.

Now, after several months of teeth gnashing, the U.S. government and the EU recently announced the launch of “EU-U.S. Privacy Shield,” the new and improved Safe Harbor program, designed to meet the concerns raised by the ECJ and others (22 PRA, 2/3/16). While lots of uncertainty remains (mainly how will the court address this new program in the face of the expected new lawsuit challenging it and how various countries will respond), companies in all industries are evaluating whether to participate in the new Privacy Shield program as a means of ensuring the appropriate ability to transfer data from the EU to the U.S.

What does this all mean for the health-care industry? What are the key areas for consideration? And will this program help or hurt privacy rights for individuals and the ability of the health-care system to improve treatment and make the system more efficient? While we have lots to continue to digest and analyze about the Privacy Shield program, and there is both an “annual review” process for the program (with the primary privacy oversight group in Europe already staking out its ground to make this a meaningful review) and the likely need for additional change based on the new EU privacy law that is coming into effect in 2018, the health-care industry needs to be thinking today about how this program will affect both individual businesses and the overall operation of the health-care system.

The Program Will Be Challenging for Everyone

The primary goal of the Privacy Shield program is to improve on the privacy protections that were created for the Safe Harbor program. This means that it will be harder to meet the challenges of the Privacy Shield program, individuals will have more rights, overall monitoring and compliance will be more significant, and the risks of enforcement will be greater. This does not at all mean that companies should not pursue Privacy Shield certification, but it does mean that this is a meaningful effort that will require a significant review of a company's overall privacy activities and protections.

There Will Be Additional Challenges if You Were Not Part of the Safe Harbor Program

For the companies that participated in the Safe Harbor program, the Privacy Shield certification will follow many of the same steps, with additional requirements and the broader need for stringent assessment and oversight. It is a significant modification to Safe Harbor, but not a wildly different framework. For those companies that did not participate in the Safe Harbor, however, the Privacy Shield will be a significant mountain to climb. It will require companies to review overall data collection activities across the business, to identify what personal data is collected from the EU, how it is used, and to whom it is disclosed. It will require the development of specific kinds of policies and procedures, a detailed privacy notice, new contracts with vendors and an overall monitoring program to evaluate the privacy activities on an ongoing basis. Many companies will undertake this effort, and will find it beneficial for the overall business activities. But this initial consideration of whether the Privacy Shield is worth the effort for your company is a significant question that will require thoughtful analysis and a meaningful assessment of available alternatives.

Privacy Shield Won’t Work for Health Insurers

One of the limits of the Privacy Shield program is that only companies subject to regulation by specified U.S. government...
agencies are eligible for the program. These agencies—for now—are limited to the Federal Trade Commission (FTC) and the Department of Transportation. That means that there are substantial gaps in who can even participate in this program. One major gap for the health-care industry involves insurers—who are subject to state regulation and generally are not subject to enforcement from the FTC (insurers may be able to participate as employers for their own employee data if needed). So, to the extent that U.S. health insurers need to receive individual information from the EU—and many will, related to vendors, travelers, international operations or the like—the Privacy Shield does not present a means of accomplishing that transfer. There may be other approaches, but this one will not work for health insurers.

Non-Profits Also Will Have Issues

Also, the FTC’s jurisdiction generally does not extend to non-profit organizations. So, for the many hospitals and other entities that operate—in a corporate sense—as non-profits, the Privacy Shield also is not an option. While many of these non-profits may be smaller organizations that do not engage in meaningful data transfer with the EU, this obviously will impact larger health-care providers who operate on a non-profit basis.

Obtaining Consent Will Be More Difficult

One of the alternatives to the Privacy Shield is to obtain the consent of the individual to the transfer. In addition, one of the Privacy Shield requirements includes the need for consent for certain data transfer in certain situations. In general, the intersection between the new EU data protection rules (stemming from the General Data Protection Regulation (GDPR) going into effect in 2018) and the Privacy Shield is to make consent a more challenging option in every respect. Also, the intersection of these two developments will both expand the situations where consent may be needed, and increase the complexity of obtaining meaningful consent consistent with the applicable rules.

Sensitive Information

At the same time, consent requirements and data protection rules generally are more significant across the board for “sensitive” information, which includes health-care information. There is some subtlety to this point, as what is considered “health information” may be more specific and narrow under these rules than the term would be under HIPAA, where any information about an identified patient or insured (including name, address and the like) is considered “protected health information” even if it says nothing specific about someone’s health. But, it will certainly be much more challenging in general to transfer health information than other “less sensitive” information about individuals. Under the Privacy Shield provisions, certifying organizations “must obtain affirmative express consent (opt in) from individuals” if this “sensitive” information is to be disclosed to a third party or used for purposes beyond which it was originally collected. While this will not require consent for disclosures to business associates, there will be interesting and challenging questions about the variety of other third parties who may receive information (and the purposes for these disclosures), particularly in the context of HIPAA’s long list of “public policy” disclosures (e.g., health care oversight, public health, litigation, etc.).

Research

One of the key areas for data transfer involves health-care research, where information about patients in a broad range of geographic settings may be useful for research projects in the U.S. and elsewhere. Although the Privacy Shield includes some specific provisions related to research (and consent often may be a viable option in research settings), the need to develop appropriate transfer mechanisms for research activities will be a significant challenge. In addition, while the Privacy Shield provisions recognize the usefulness of personal data for beneficial research, the primary ability to use personal data obtained for one study in another context is dependent on whether “appropriate notice and choice” have been provided in the first instance.

Privacy Shield Certification May Complicate Business Associate Relationships

One of the key expanded protections from the Privacy Shield involves the “onward transfer” provision, which regulates how data that is transferred to the U.S. is subsequently transferred by the recipient to other entities, in the U.S. or elsewhere. These onward transfer requirements require specific kinds of contractual requirements and ongoing monitoring of vendors and others who receive information. The Privacy Shield is simply different than the contractual requirements for business associates under HIPAA. This may require companies to re-evaluate existing agreements, to modify them consistent with the onward transfer provisions, and to adopt more aggressive monitoring of vendors beyond the existing HIPAA provisions.
De-Identification issues

One alternative to any data transfer program is to ensure that the data being transferred is not subject to existing data protection rules. Under HIPAA, this kind of action would involve “de-identification” of protected health information subject to the specific HIPAA requirements. Although the Privacy Shield does incorporate the idea of individually identifiable information (as does the new GDPR), it provides a less certain path to making information “de-identified.” Therefore, companies wishing to bypass Privacy Shield requirements due to de-identification will need to re-evaluate how to ensure appropriate de-identification consistent with the EU and Privacy Shield standards, which are different than the existing HIPAA framework.

Alternative/Different Enforcement

The ability to certify under the Privacy Shield is dependent on the ability of the Federal Trade Commission to take enforcement action against an entity for violation of the Privacy Shield commitments. Therefore, for any health-care entity subject to the HIPAA rules as a covered entity or business associate, the FTC will become an independent enforcement agency in connection with the commitments made under the Privacy Shield (which may be similar to and overlap with HIPAA, but which are different). Although HIPAA-regulated entities should be aware of the FTC’s view that it already can take action against HIPAA entities based on the FTC’s own privacy and security principles (as they did in the longstanding and controversial LabMD Inc. case (228 PRA, 11/27/15), the Privacy Shield will make the FTC’s enforcement ability explicit, and will define the standards that underlie any enforcement activity. The Department of Commerce also will have jurisdiction to engage in proactive audits and to evaluate complaints against participating companies.

Conclusion

Overall, the Privacy Shield program will have a substantial impact on how many U.S. companies will be able to receive data from Europe, and on how this data can be subsequently transferred to other recipients and for other purposes. Some companies in the health-care industry (e.g., drug manufacturers, pharmacies, larger health-care providers, for example) may find the Privacy Shield to be a useful and viable option; others will be unable to participate or will find the compliance challenges too broad and complicated. In this event, there may be other options, and companies will need to consider these alternatives based on their own situation. In any event, the Privacy Shield will provide a new path to ensure data transfer from Europe for many companies, but also will create new compliance challenges and new avenues for complicated analysis of how best to ensure the appropriate use and disclosure of health-care information.
New EU-U.S. Data Transfer Pact May Face Court Challenges

BNA Snapshot

• Recently approved trans-Atlantic data transfer pact has stronger obligations than its predecessor
• Companies need to plan and understand how they will fulfill Privacy Shield's obligations on ongoing basis

By Jimmy H. Koo

July 21 — U.S. companies that do business in the European Union should view the text of the new EU-U.S. Privacy Shield data transfer agreement as a guideline for compliance, privacy professionals told Bloomberg BNA.

The Privacy Shield places stronger obligations than its predecessor, the invalidated U.S.-EU Safe Harbor framework that was relied on by over 4,400 U.S. companies and tens of thousands of EU companies to legally transfer personal data to the U.S. (15 PVLR 1478, 7/18/16).
“It's good to have a new mechanism in place to mitigate risk and increase business confidence,” Omer Tene, vice president of Research and Education at the International Association for Privacy Professionals, told Bloomberg BNA.

However, the Privacy Shield may still be challenged in the EU courts and may not pass muster under the EU General Data Protection Regulation (GDPR), which takes effect May 2018, the privacy pros said. For that reason, companies should be ready to respond accordingly, they said.

Matthew Fawcett, senior vice president and general counsel of NetApp Inc., told Bloomberg BNA that the Privacy Shield was written to address requirements under the EU data protection directive, not the more stringent GDPR, which takes effect May 25, 2018 (15 PVLR 963, 5/9/16). Tene agreed.

Once the GDPR comes into effect, “complying with Privacy Shield obligations may no longer be enough,” Tene said.

New Requirements and Obligations

Liisa M. Thomas, partner and chair of Privacy and Data Security Practice at Winston & Strawn in Chicago and London, told Bloomberg BNA that the “Privacy Shield places many procedural burdens on organizations.”

“While they may be achievable, companies who are moving forward with the Privacy Shield would be well served to have a playbook or other internal guidance document in place to make sure they understand how they will continue to fulfill the Shield's obligations on an ongoing basis,” she said.

According to Fawcett, there are more similarities than differences between the Privacy Shield and the Safe Harbor. Nonetheless, the Privacy Shield requires stronger monitoring and enforcement by the Commerce Department and the Federal Trade Commission, including “stronger cooperation with European Data Protection Authorities,” Fawcett said. It also “tightens conditions for cross-border transfers and requires clear safeguards and transparency obligations on U.S. government access,” he said.

Annex VI of the Privacy Shield limits governmental access to data for intelligence collection purposes. “The U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms,” Fawcett said.

Further, under Annex A, the U.S. must establish an ombudsman within the State Department who will follow up on complaints and inquires by individuals.

The Privacy Shield also provides EU citizens with several redress possibilities, including a free alternative dispute resolution mechanism under Annex II Art. II.1.a.ix, as well as an enforceable arbitration mechanism under Annex II, Art. II.1.9.xi.

According to Thomas, “one of the more striking provisions is the ability for individuals in the EU to take advantage of arbitration provisions built into the Privacy Shield program” that can be used after exhausting other dispute resolution options.

In addition to governmental commitments and obligations, the Privacy Shield also imposes certain requirements that companies need to be aware of.

Under Annex II, Art. III.7, companies must have “measures in place to ensure that their privacy statements are true, either through internal verification or using an outside company to perform compliance reviews,” Thomas said.

Tene said that companies must “obtain consent from Europeans before sharing data with third parties, including affirmative express consent to share sensitive information.” The Privacy Shield also requires “sub processors to commit to the same level of protection and monitor their compliance with these rules,” he said.
Companies “will have to develop a separate privacy policy related to the collection and handling of employee data,” Fawcett said.

Fawcett recommended that companies provide employees with “clear and transparent notices of data processing.” Companies should check with “work councils and trade unions” about data transfers to the U.S. and confirm that EU subsidiaries comply with local requirements and restrictions, he said.

**Challenges and Uncertainties**

Tene said that despite the new obligations, improved protections and availability of redress, “it remains to be seen” whether the changes are sufficient to survive ECJ scrutiny.

Some privacy advocates, including European Data Protection Supervisor Giovanni Buttarelli, have similarly argued that the Privacy Shield will be vulnerable to being thrown out by the ECJ (15 PVLR 1161, 6/6/16).

“The court may be concerned about the legal weight of the commitments of the U.S. government, which appear in side letters and not in law,” Tene said.

Fawcett agreed. Even with the negotiated changes, there isn’t “specific information regarding how the U.S. plans to implement the new requirements agreed to in the Privacy Shield,” he said.

However, EU Commissioner for Justice, Consumers and Gender Equality Vera Jourov recently urged skeptical lawmakers “not to simply dismiss this mechanism before it has even been put to the test” (15 PVLR 1479, 7/18/16).

Tene said that “with additional court challenges on the horizon, Brexit destabilizing the EU, and an avalanche of data flowing constantly across borders, the European framework purporting to impose border checks on data flows is increasingly strained.”

Fawcett urged that “companies need to think ahead and decide whether or not embracing Privacy Shield makes sense for them.”

To contact the reporter on this story: Jimmy H. Koo in Washington at jkoo@bna.com

To contact the editors responsible for this story: Donald G. Aplin at daplin@bna.com; Daniel R. Stoller at dstoller@bna.com

For More Information

The European Commission and the U.S. Department of Commerce-approved updated version of the EU-U.S. Privacy Shield was green lighted by a regulatory committee of EU countries July 8 and will be formally adopted and finalized the following week, the authors write as they discuss the outlines of the new data transfer pact.

Françoise Gilbert is a partner at Greenberg Traurig LLP in Palo Alto, Calif. She is the author and editor of the two-volume treatise Global Privacy and Security Law, which analyzes the data protection laws of 68 countries.

Marie-José van der Heijden is an associate at Greenberg Traurig LLP in Amsterdam.

The European Commission and the U.S. Department of Commerce have agreed on a new draft of the Privacy Shield agreement (Shield v 2.0). The documents that form the Privacy Shield v 2.0 are an updated version of those that were published in late February 2016. After its publication, the initial draft of the Privacy Shield agreement was strongly criticized by the Article 29 Working Party, the European Data Protection Supervisor, and the European Parliament, preventing its ultimate adoption. See, e.g., Greenberg Traurig Alert “Thumbs Down to Draft EU-U.S. Privacy Shield,” April 14, 2016.

The currently available unofficial version of the final Privacy Shield v 2.0 documents appears to be largely based on the February 2016 version. However, the documents do contain more provisions, clarify many issues, and introduce some additional requirements. The primary changes are found in the Draft Commission Implementing Decision Regarding the Adequacy of the Protection Provided by the European Union-U.S. Privacy Shield (the Decision).

Among other things, the Decision clarifies that the new Privacy Shield also applies to the transfer of personal data from Iceland, Liechtenstein and Norway, and not only from the EU Member States. It also clarifies that certified companies will be required to include a provision in onward transfer contracts obligating the recipient of personal data to notify the Privacy Shield-certified company if the recipient can no longer provide the same level of protection as required by the Privacy Shield Principles (Principles). Certified companies will also be required to include an express obligation in contracts to require the deletion or de-identification of personal data after they are no longer relevant for the identified purposes of processing or for compatible purposes, with the exception of processing for public interests. The Decision also clarifies that the Privacy Shield will be administered by the U.S. Department of Commerce, and will be enforced by the Federal Trade Commission and the Department of Transportation.

Scope of Application

Like the EU-U.S. Safe Harbor, its predecessor, the EU-U.S. Privacy Shield will be based on a system of self-certification by which U.S. organizations commit to the Principles. The Principles will apply to both data controllers and data processors, but data processors must also be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under the Principles.

The updated Decision clarifies that the Principles will apply solely to the processing of personal data by a U.S. organization in so far as the processing by such organization does not fall within the scope of European Union legislation. It is worth noting
that a U.S. company that processes personal data of residents of the European Union or European Economic Area (EEA), and whose activities fall within the scope of Article 3 the General Data Protection Regulation (GDPR) should not assume that its self-certification under the Privacy Shield will be sufficient to demonstrate its compliance with all provisions of the GDPR that apply to its operations.

Article 3 of the GDPR provides that the activities of a data controller that is not established in the European Union fall within the scope of application of the GDPR when these processing activities are related to (i) the offering of goods or services to Individuals in the EU irrespective of whether a payment is required; or (ii) the monitoring of the behaviors of individuals when that behavior takes place in the European Union.

**Transition Period**

The updated Decision also clarifies that while the general rule will be that the Principles apply to a U.S. business immediately upon filing of the self-certification documents with the U.S. Department of Commerce, there will be an exception for cases where an organization has a pre-existing relationship with third parties.

If an entity files its self-certification documents within two months from the day when the Privacy Shield becomes effective, it will be granted a nine-month grace period to bring its commercial relationships in conformity with the rules applicable under the Accountability for Onward Transfer Principle. During that transition period, the organization must allow data subjects to opt-out, and when personal data is transferred to a third party acting as an agent, it must ensure that the agent provides at least the same level of protection as required by the Principles.

**Updated Analysis of the Privacy Principles**

The updated Decision contains numerous clarifications of its prior analysis of the Privacy Principles that was included in the February 2016 version of the Privacy Shield documents.

**Data Integrity and Purpose Limitation**

The Data Integrity and Purpose Limitation Principle provides that personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete and current. The Shield v 2.0 clarifies that organizations must ensure that personal data is reliable for its intended use, accurate, complete and current.

**Choice**

Under the Choice Principle, data subjects may opt-out if their personal data is to be disclosed to a third party or used for a materially different purpose. The updated Decision clarifies that where a new purpose is materially different, but still compatible with the original purpose, data subjects also have the right to opt-out or object. In addition, it clarifies that special rules will apply to the use of personal data for direct marketing purposes, to allow individuals to opt-out at any time.

**Accountability for Onward Transfers**

The Accountability Principle states that transfers of personal data will be possible only: (i) for limited and specified purposes; (ii) on the basis of a contract or similar arrangement within a corporate group; and (iii) if that contract provides the same level of protection as guaranteed by the Principles. The updated Decision clarifies that the obligation to provide the same level of protection as required by the Principles must apply to all parties involved in the processing of the data so transferred, irrespective of their location, when the original third party recipient itself transfers the data to another third party recipient, for example a subprocessor.

**Access; Correction**

The Access Principle grants data subjects the right to obtain confirmation from an organization whether that organization is processing personal data related to them, and to have the data communicated within reasonable time. The updated Decision clarifies that data subjects will also have the right to correct, amend, or delete personal data that is inaccurate or has been processed in violation of the Principles. This right can be exercised without justification, and only against a non-excessive fee.

The additional comments address the use of data to make automated decisions that affect an individual. Such an automated individual decision may significantly affect a person and is based on automated processing of personal data with a view to evaluate that specific person. The updated Decision points to the significant discrepancies between the U.S. and EU regimes in this respect. U.S. laws offer specific protection in certain areas such as when data is used for making decisions regarding
employment offers, or in connection with credit or lending decisions. While acknowledging that the use of automated processing as a basis for making decisions and such evaluations that relate to different personal aspects as work performance, creditworthiness, reliability and conduct is increasing, the Decision indicates that the U.S. and EU now have agreed that a dialogue on profiling and automated decisions and evaluations will take place during the annual reviews of the implementation of the Privacy Shield agreement. This future dialogue should resolve the issue posed by Article 15 of Directive 95/46/EC and Article 19 of Regulation (EC) No. 45/2001. These provisions lay down the right for individuals to object to such decisions that are based solely on automated means about them, unless certain conditions are fulfilled or appropriate safeguards are in place.

**Recourse, Enforcement and Liability**

The updated Decision clarifies that the Principles will apply solely to the processing of personal data by a U.S. organization in so far as the processing by such organization does not fall within the scope of European Union legislation.

The Recourse, Enforcement and Liability Principle requires organizations to provide robust mechanisms to ensure compliance with the other Principles and recourse for EU data subjects whose personal data has been processed in a non-compliant manner, and includes effective remedies.

The additional comments provided in the updated Decision focus on enforcement. It is expected that organizations that have failed to deal appropriately with complaints will be subject to the investigatory and enforcement powers of the Federal Trade Commission, the Department of Transportation or another U.S. authorized statutory body that must effectively ensure compliance with the Principles. The updated Decision contains a lengthy analysis of the Recourse, Enforcement and Liability Principle that details the eight levels of redress—which must be addressed in a specific sequence—of the escalation procedure that will be available to EU residents who would have complained about the handling of their data, and would not have obtained resolution to their satisfaction.

**Increased Focus on Transparency and Oversight**

A significant portion of the analysis laid out in the Decision focuses on oversight and enforcement mechanisms, to address complaints and concerns that the United States did not aggressively enforce compliance with the Safe Harbor Principles. In its supplementary analysis, the Decision observes that the Shield provides for oversight and enforcement mechanisms in order to verify and ensure that U.S. self-certified organizations comply with the Principles, and that any failure to comply is adequately addressed.

Among the new measures introduced by the Privacy Shield, the U.S. Department of Commerce is tasked with monitoring whether the organizations listed on the Privacy Shield list as having self-certified are current in their obligations, and, if they are not, ensuring that they have returned or deleted the personal data that they received under the Privacy Shield. The Department of Commerce is also tasked with monitoring any false claims of participation in the Privacy Shield, and improper use of the Privacy Shield certification mark.

The Decision also clarifies that, on an on-going basis, the Department of Commerce will conduct ex officio compliance reviews of self-certified organizations. Those compliance reviews will include detailed questionnaires and investigations when it has received a specific complaint, when an organization does not provide satisfactory responses to its inquiries or where there is credible evidence suggesting a failure to comply with the Principles.

**Access by U.S. Public Authorities**

One of the key points of friction between the U.S. and the EU has been the nature and scope of the U.S. laws that regulate access that U.S. public authorities have to personal data of EU citizens stored on servers within the jurisdiction of U.S. public authorities.

The updated Decision supplements the pre-existing analysis of the applicable U.S. laws. It clarifies that the EU Commission has analyzed U.S. law and determined that it contains a number of limitations on the access to, and use of, personal data transferred to the United States for national security purposes, as well as sovereign and redress mechanisms that provide sufficient safeguards for those data to be effectively protected against unlawful interference and the risk of abuse. It concludes that in the Commission’s opinion, the current U.S. laws satisfy the standard set by the

**After the opinion delivered by the Article 29 Working Party earlier this year, the European Commission directly assured it would incorporate a number of recommendations by the data protection authorities.**
The draft of the Privacy Shield further states that “bulk collection will only be authorised exceptionally where targeted collection is not feasible, and will be accompanied by additional safeguards to minimise the amount of data collected and subsequent access (which will have to be targeted and only be allowed for specific purposes).” The definition of “feasible” is left to practice.

Next Steps

The Privacy Shield should provide legal certainty to corporations that transfer personal data from the EU/EEA to the U.S. Under current EU national data protection laws—and later under the General Data Protection Regulation—personal data can only be sent to the U.S., a non-EU country, if the U.S. guarantees EU residents a level of legal protection that is essentially equivalent to that they receive in the EU. As this is not the case, the Privacy Shield was needed. However, the agreement also needs an adequacy decision. An adequacy decision is a decision adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC which establishes that a third country ensures an adequate level of protection of personal data by reason of its domestic law or the international commitments it has entered into. Then, personal data can be transferred from the 27 Member States and the three EEA countries to the U.S., without additional safeguards (adequacy decisions were issued for several countries throughout the world, for example, Switzerland, Canada, Argentina, Guernsey, Isle of Man, Uruguay, Israel, New Zealand and the transfer of Air Passenger Name Record (PNR) data to the U.S. Bureau of Customs and Border Protection).

Such adequacy decisions are adopted pursuant to the comitology procedure, which involves the following steps: (i) a proposal from the Commission, (ii) an opinion of the Article 29 Working Party, (iii) an opinion of the Article 31 Committee, and (iv) the adoption of the decision by the College of Commissioners. At all times, the European Parliament and the Council can request the Commission to maintain, amend or withdraw the adequacy decision if they view its act exceeds the implementing powers provided in the Directive.

After the opinion delivered by the Article 29 Working Party earlier this year, the Commission directly assured it would incorporate a number of recommendations by the data protection authorities. The proposal was sent both to the Article 31 Committee and to the European Parliament, but the latter cannot block it. The Article 31 Committee that consists of representatives of all 28 Member States and the Commission voted on the Privacy Shield early July 8. The Article 31 group had to vote in favor by a qualified majority of 16 EU Member States that represent at least 65 percent of the EU population. On Monday, the European Commissioner Jourová will inform the Civil Liberties, Justice and Home Affairs committee of the European Parliament on the state of play. It is expected Jourová and U.S. Secretary of Commerce Penny Pritzker will sign the framework agreement at the beginning of next week.
Global Perspectives: Brexit's Impact on International Data Transfers

After the people of the U.K. voted to leave the European Union, any decision on the future of data protection law in the U.K. will be influenced by the agreements that the U.K. reaches with the EU once it leaves. The author lays out the five possible routes that the U.K. may take. For most organisations, the prudent course of action based on the information available would be to continue with preparations for the General Data Protection Regulation as if Brexit had never happened, the author writes.

By Rohan Massey

Rohan Massey is a partner at Ropes & Gray LLP in London and leads the firm's privacy and data security practice in Europe.

On June 23, 2016 the people of the U.K., by a slim margin of 52 percent to 48 percent, voted to leave the European Union, a move better known as "Brexit" (123 PRA, 6/27/16). This somewhat surprising result has created turmoil in the financial markets, resignations from the government and the opposition party, and great uncertainty as we look for the answer to the question “what happens now”?

The U.K.'s exit from the EU will not be immediate; we need to give notice to leave formally, commencing the Article 50 exit process. Even initiating this process seems some time off and, once notice is served, there is a minimum two year period under Article 50 before a Member State can leave the EU. For this reason, any final exit by the U.K. is unlikely to occur before late 2018 or early 2019.

So in a year that has seen the U.S.-EU Safe Harbor Framework invalidated by the Court of Justice of the European Union (CJEU); the new EU General Data Protection Regulation (GDPR) adopted and scheduled to take direct effect from May 25, 2018; the draft EU-U.S. Privacy Shield published and criticised by the Article 29 Working Party, the European Parliament and the European Data Protection Supervisor; and the U.K. actually voting to leave the EU, where does this leave the U.K. with regard to international data flows, going forward?

For Now—Keep Calm and Carry On

The U.K. Information Commissioner's Office (ICO) made clear in its press release of June 24, 2016, that the Data Protection Act 1998 (DPA) remains the law of the land and all processing of personal data must be undertaken in accordance with the DPA. An updated statement on July 1, 2016 confirmed that reform of U.K. data protection law remains necessary (although the precise form this reform will take is, as yet, unclear). The DPA allows for personal data to be transferred freely to the European Economic Area (EEA) member states and those countries covered by European Commission findings of adequacy. The DPA also provides that consent, model clauses, binding corporate rules (BCRs) and self-assessed adequacy may be used to legitimise international transfers of personal data to countries outside the EEA, which are not covered by an adequacy decision. In addition to this, although the Safe Harbor framework is no longer a valid means for legitimising data transfers to the U.S., as recently as February 2016, the ICO's position remains that it “… will not be seeking to expedite complaints about Safe Harbor while the process to finalise its replacement remains ongoing and businesses await the outcome.”
**What Are the Future Options?**

Any decision on the future of data protection law in the U.K. will be influenced by the agreements that the U.K. reaches with the EU once it leaves. Possible options are set out below.

1. **Implement the GDPR (or an Equivalent)**

Following exit from the EU, as it has already agreed the text of the GDPR as a member state of the EU, the U.K. may decide to implement the GDPR and repeal the DPA, by way of national legislation. This option should assist in the facilitation of trade links with the EU going forward and remove at least one barrier. If the U.K. remains outside the EEA, but implements the GDPR (or something very similar) then it is likely that a finding of adequacy by the European Commission would follow.

2. **The Norwegian Model**

If the U.K.’s relationship with the EU was agreed along the same lines as Norway’s current membership of the EEA, then the U.K. would need to adhere to the GDPR and take steps to implement it with effect from the end of the Article 50 process. Under this option, data transfers from the U.K. across the EEA would be permitted freely and the U.K. would also benefit from the European Commission's findings of adequacy in respect of international jurisdictions that are deemed to provide an adequate level of protection for personal data. The U.K., together with all other EEA Member States, would also be able to avail itself of the protections offered by the proposed EU-U.S. Privacy Shield, once adopted, regarding personal data transfers to the U.S.

3. **The Adequacy Route**

If the U.K. were to leave the EU and not become a member of the EEA, it would be treated as a third country by the EU for the purposes of international personal data transfers. As noted above, if the U.K. chose to implement a new regime based on the GDPR principles it is highly likely that the Commission would find the protection afforded to personal data by the U.K. to be adequate and add the U.K. to its “white-list,” as it has done for countries including Argentina, Israel and Switzerland under Data Protection Directive (95/46/EU).

However, were the U.K. to retain the DPA and not implement an equivalent to the GDPR, then it is possible that no finding of adequacy would be made on the grounds that the GDPR is more robust in its protection and requirements than the Directive (and therefore the DPA). Furthermore, some may view the U.K.’s historical interpretation, implementation and pragmatic approach in respect of the Directive as offering a lower standard of protection than that which will be required under the GDPR. In this scenario, all personal data transfers to the U.K. from the EEA would need to be legitimised by model clauses, BCRs, consent or any of the other safeguards or derogations available under the GDPR, with the U.K. controller or processor being the data importer in each case. This may require many organisations to review commercial contracts and data sharing arrangements that are currently in place to ensure ongoing compliance.

4. **An EU-U.K. Privacy Shield?**

If the U.K. decided to remain outside the EEA and not implement the GDPR, intending to rely on the DPA going forward, as noted above any such regime is unlikely to be sufficient for a Commission adequacy finding under the GDPR. In addition, the Investigatory Powers Bill (IPB), which is currently before the U.K. Parliament, may make a finding of adequacy even less likely. This is because, as currently proposed, the IPB would allow bulk personal datasets to be collected for purposes of national security without regard to data protection compliance.

In the absence of an adequacy finding by the Commission, one possibility would be to implement a “Privacy Shield” type arrangement between the U.K. and the EU similar to the proposed EU-U.S. Privacy Shield. However, the proposed terms of the IPB may mean that the U.K. will find itself in a similar position to the one that the U.S. is in at present. There would need to be careful negotiations as to the form of arrangement allowing for international data flows to the U.K.
5. A Dual System?

There is a final option in which the DPA remains in force and is applied to all international data flows from the U.K. outside the EEA when a controller is established in the U.K., where the processing of personal data takes place exclusively in the U.K. and the processing is limited to U.K. citizens. For all other international transfers the GDPR would apply. Among other things, this could allow the U.K. to assist small businesses. Although there may be some merit in this proposal, the complexity of administration makes this a very impractical solution.

So there we have it, a number of options, but no clear leader as yet. As the clock ticks ever closer to May 2018, a decision and clarity on these points would be welcome sooner rather than later. For most organisations, the prudent course of action based on the information available would be to continue with preparations for GDPR as if Brexit had never happened.
BNA Snapshot

**Brexit, EU Single Market and Privacy**

**Development:** Following its decision to leave European Union, U.K. faces another tough decision with privacy implications about participation in European single market.

**Takeaway:** Within single market, EU General Data Protection Regulation would apply to U.K.; outside single market, U.K. would have to demonstrate adequacy of its privacy regime.

By Stephen Gardner

June 30 — The post-Brexit U.K. faces a tough decision with privacy implications on whether it should continue to participate in the unified European economy despite voting to leave the European Union.

Within the single European market, the EU would require the U.K. to follow the new EU General Data Protection Regulation ((EU) 2016/679) (GDPR), outside the market the U.K. would have to demonstrate the adequacy of its independent privacy regime in order to lawfully accept personal data from the remaining 27 EU countries.

The departure from the common market might also put the U.K. at risk for participation in trans-Atlantic data transfer deals, including the nascent EU-U.S. Privacy Shield program. It might also diminish the U.K. privacy office's ability to influence European privacy and data security developments.

Companies that handle personal data likely hope the U.K. will stay in the single market. This would allow more-or-less business as usual. But it would require the U.K.’s political leaders to make some compromises, privacy attorneys working in the EU told Bloomberg BNA.

**General Data Protection Regulation**

The U.K.’s continued participation in the single market would allow the GDPR to take full effect in the U.K. Negotiators Dec. 15, 2015 concluded nearly four years of talks on final text of the GDPR to replace the EU's now over 20-year-old Data Protection Directive (95/46/EC) (14 PVLR 2289, 12/21/15). It will apply for all EU countries as of May 25, 2018 (15 PVLR 963, 5/9/16).

Jan Philipp Albrecht, the German Green lawmaker who was the European Parliament's lead negotiator on the GDPR, told Bloomberg BNA June 29 that he “very much” hopes the U.K. stays in the single market.

The U.K. had been “from the beginning very supportive of a new data protection framework that creates more legal certainty. All in all, it would be a real pity if the U.K. does not benefit from that,” Albrecht said.

**Privacy Shield at Risk?**

Companies would likely prefer the U.K. to stay in the single market because the alternative would be fraught with difficulty and uncertainty.

Ann LaFrance, partner co-leader of Data Privacy & Cybersecurity practice at Squire Patton Boggs in London, told Bloomberg
BNA June 29 that "under an independent model where the U.K. renegotiates its trade relationships, the U.K. would have to negotiate their own Privacy Shield-type arrangements with the EU, or obtain third-country status from the European Commission."

"Under an independent model where the U.K. renegotiates its trade relationships, the U.K. would have to negotiate their own Privacy Shield-type arrangements with the EU, or obtain third-country status from the European Commission."

Ann LaFrance, Partner, Squire Patton Boggs, London

The EU-U.S. Privacy Shield is a proposed framework for trans-Atlantic transfers of personal data to replace the invalidated U.S.-EU Safe Harbor framework (15 PVLR 269, 2/8/16). The European Court of Justice—the EU's top court—Oct. 6, 2015 invalidated the Safe Harbor on the basis that it failed to sufficiently protect to the privacy of EU data subjects (14 PVLR 1825, 10/12/15)

But in putting in place such an arrangement, the U.K. could face similar problems to those experienced by the U.S. over Safe Harbor.

Jorg Hladjk, of counsel with Jones Day in Brussels, told Bloomberg BNA that there would have to be "a discussion of whether there is really equivalent protection" in the U.K. to that offered in the EU under the GDPR.

For the U.K. this would mean that "if the GDPR no longer applies, they will have to come up with something that's very close," Hladjk said.

Proving Adequacy

Albrecht said that proving the adequacy of the privacy protections offered by the U.K. in the event the U.K. opts out of the single market might be a "hard task."

The European Commission, the EU's executive arm, makes decisions on the adequacy of third country data protection regimes. The decisions, which must be approved by the European Parliament and EU countries represented in the Council of the EU, allow personal data to be transferred freely to countries judged to have privacy protections in place to adequately protect the privacy of data transferred there.

Even if the U.K. went the adequacy determination route, it would likely need to amend its Data Protection Act 1998 to largely incorporate the main privacy points of the GDPR. If it didn't do so, the U.K. law might be "seen as rather weak" and therefore potentially inadequate, Albrecht said.

"There are several points of criticism" of the U.K. Data Protection Act, including its provisions on consent, the right of erasure of personal data and enforcement, Albrecht said.

LaFrance said that in such a situation, the commission would be "likely to require the U.K. to put laws more stringent than the Data Protection Act in place as a condition of recognizing the adequacy of the U.K.'s data privacy regime."

Philip James, a technology partner at Sheridans in London, told Bloomberg BNA that a "sensible approach" would involve the U.K. demonstrating it has adequate privacy safeguards in place by "incorporating the GDPR into U.K. law by means of a specific U.K. statutory instrument."

Surveillance Concerns

A future commission adequacy decision on the U.K. might be under threat on similar grounds to those that invalidated Safe Harbor. It may be difficult for the U.K. to prove that the personal data of EU citizens aren't subject to unwarranted surveillance by U.K. intelligence services.

The U.K.'s secretive Government Communications Headquarters (GCHQ) was cited by Edward Snowden, the former employee of a U.S. National Security Agency contractor who leaked information about government surveillance programs, as indulging in mass electronic surveillance.

Albrecht said that if the U.K. steps outside the European single market, its data protection regime would be "judged on all those intelligence issues."
Snowden's disclosures and the invalidation of Safe Harbor led to an upgrading of privacy protections in the U.S. to guard against unwarranted government surveillance, Albrecht said. “I don't see that in the U.K. at the moment,” he said.

Hladjk said that pending cases before the European Court of Human Rights, which isn't an EU court, alleging that surveillance by the U.K. intelligence agencies violates privacy rights, might be taken into account in any future adequacy decision relating to the U.K.

European Economic Area

Considering the potential difficulties that the U.K. may face in earning a commission adequacy decision if it steps outside the single market, the common sense option would seem to be to stay in the single market and be subject to the GDPR, attorneys said.

Campaigners for the U.K. to leave the EU made contradictory promises about remaining in the single market. Some suggested staying in the single market while not accepting some of its basic principles, including the free movement of people.

The GDPR will apply to the EU and to three non-EU countries—Iceland, Liechtenstein and Norway—that are members of the European Free Trade Association (EFTA) and that adhere to the European Economic Area (EEA) Agreement, which extends the single market beyond the EU.

EFTA senior officer Tore Grønningsæter told Bloomberg BNA that the three countries would be required to transpose the GDPR into their national legal codes, though this could be done by a simple reference to the final text of the regulation.

EEA countries could in principle refuse to adopt an EU law, but the consequence could be suspension of single market participation and, after twenty years and about 10,000 laws from the EU, “we haven't done a single veto yet,” Grønningsæter said.

It remains unclear whether U.K. politicians would be able to tolerate such a system. The U.K. had joined the EU “principally to be a member of the single market. Why move out of that and into it again without voting rights?” Grønningsæter said.

Less Influence for U.K. Privacy Office?

Single market participation for the U.K. without EU membership would also have implications for the U.K. privacy regulator, the Information Commissioner's Office.

Kim Ellertsen, head of the legal department at the Norwegian Data Protection Authority, told Bloomberg BNA that the Norwegian DPA has only observer status in the Article 29 Working Party of EU data supervisors. The Art. 29 Working Party will be replaced by the European Data Protection Board when the GDPR takes effect.

In terms of participation in the preparation of guidance on the GDPR, for example, “we're doing things all the other DPAs are doing but at smaller scale,” Ellertsen said.

The Norwegian DPA also has little influence over frameworks such as Privacy Shield, though if the European Commission approves Privacy Shield “it will be valid in Norway through the EEA Agreement,” Ellertsen added.

To contact the reporter on this story: Stephen Gardner in Brussels at correspondents@bna.com

To contact the editors responsible for this story: Donald G. Aplin at daplin@bna.com; Jimmy H. Koo at jkoo@bna.com
Companies Should Focus on EU Privacy Regime Post-Brexit

BNA Snapshot

**Development**: U.K. votes in referendum to leave European Union.

**Next Step**: Brexit will have little impact on data privacy and companies should continue to focus on implementing the European Union General Data Protection Regulation.

By Ali Qassim

June 24 — Companies that process or send data to European Union nations and the U.K. need to remain focused on upcoming changes to EU data protection laws despite Brexit, privacy attorneys told Bloomberg BNA June 24.

“The initial advice is for businesses to continue to focus on the internal changes they need to be making to get ready for the new EU General Data Protection Regulation (GDPR),” Rafi Azim-Khan, partner and head of data privacy in Europe at Pillsbury Winthrop Shaw Pittman LLP in London said June 24. “There should be no distraction from that given the major new fines will still be a real business risk.”

Despite the U.K.’s decision to quit the EU, U.K.-based multinational and local businesses that process or send data to any of the other 27 nations in the EU will be required to follow the GDPR.

“The situation will remain unchanged at least until there’s a formal Brexit. There’s no short-term concern” for companies operating in the U.K. and EU, Mark Prinsley of Mayer Brown LLP in London said June 24.
In the long-term, however, U.S. businesses will face a more complicated enforcement regime across the Atlantic. Instead of taking advantage of the one-stop-shop that the GDPR will establish, “U.S. companies with establishments or activities in both the U.K. and EU would—similar to the position now—face enforcement from more than one regulator,” Jonathan Kirsop, partner at Stephenson Harwood in London said.

Negotiating the U.K.’s departure from the EU is also very likely to take place after the May 25, 2018, deadline for the GDPR to come into force, James Mullock, a privacy and data protection partner at London-based Bird & Bird, said June 24.

“That's significant because it means that the U.K. will almost certainly experience life under the GDPR* despite its exit from the EU, he said.

British citizens voted to leave the EU in a June 23 referendum. The U.K. joined the then-European Economic Community in 1973.

**Withdrawal Likely Two Years Away**

Under Article 50 of the Lisbon Treaty, the U.K. will have to serve notice of its intention to exit the EU and negotiate a withdrawal agreement, Mullock said.

“Unless there is unanimous agreement to the contrary, the earliest that any withdrawal agreement will take effect under Article 50 seems likely to be two years from service of notice of the U.K.’s desire to Brexit. In reality it may take considerably longer,” he said.

Prime Minister David Cameron, in his June 24 resignation speech following the Brexit vote, said he would not trigger Article 50 until the next prime minister is chosen by October 2016.

Two potential successors—Conservative members of Parliament Boris Johnson and Michael Gove—also said June 24 that a new government shouldn't be rushed into implementing Article 50.

**Trading With EU Requires GDPR**

Mullock said any U.K. business that trades in the EU “will have to comply with the GDPR despite Brexit taking effect.”

“That's because the GDPR's many obligations will apply to organizations located anywhere in the world which process EU citizens' personal data in connection with their offer of goods or services, or their ‘monitoring’ activities—defined to pick up many online behavioral marketing activities,” he said.

A spokesman for the U.K.’s data protection authority—the Information Commissioner's Office—agreed that if any business based in the U.K. “wants to trade” with EU member states “on equal terms,” it would have to prove that it ensures an adequate level of protection for the data.

“In other words U.K. data protection standards would have to be equivalent to the EU's General Data Protection Regulation framework starting in 2018,” an ICO spokesman said June 24.

“Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to present our view that reform of the U.K. law remains necessary,” the ICO spokesman said.

**U.S. Business Impact**

U.S. companies will be regulated by separate data protection enforcement authorities in the U.K. and EU, but the U.K.’s desire to trade with EU member states and demonstrate adequacy will likely mean that the systems will be very similar or identical, Kirsop said.

“From recent discussions with privacy commissioners, it's highly likely that any updated U.K.-specific legislation will closely mirror EU data laws,” Azim-Khan said.

Moreover, U.K. and EU privacy laws are both rooted in the same traditions as the European Convention on Human Rights, Prinsley said.
It's unclear whether mechanisms for personal data transfers to the U.S. will diverge between the U.K. and EU as the EU-U.S. Privacy Shield continues to be debated.

"I don't expect the nuts and bolts of the transfer mechanisms, such as model contracts and binding corporate rules, to change much, if at all," John Drennan counsel at King & Spalding LLP's data, privacy and security group said.

Despite the similarity of any regime that emerges in the U.K., “businesses will need to closely keep an eye on not just the changes needed to deal with the GDPR, but also any exception or variation that may be introduced specifically for the U.K.,” Azim-Khan said.

**EU: ‘Dim View’ of Weak Privacy Laws**

Even if a future U.K. government decides to strike a trade deal with the EU that covers data protection, it would in theory “have free rein to choose the form of data protection laws which it introduces to update” the U.K.’s Data Protection Acts 1998 and 2003, Mullock said.

“However, recent history tells us that, when it comes to the question of data transfers, EU regulators and courts take an extremely dim view of countries which do not adopt EU-strength data protection laws, ” he said.

“Without the U.K. as an EU member state, it's possible that the EU's stance on data transfers will harden,” Drennan said, because a higher percentage of EU member states will be more skeptical about national security surveillance.

The current stand-off with the U.S. with respect to the now-invalid Safe Harbor data sharing arrangement is a case in point, Mullock said, referring to the program that was invalidated last year.

“A higher percentage of voices in the EU will now understand certain national security-related intrusions into personal data as human rights violations," Drennan added.

“Brexit could result in a ‘push and a pull’ situation that affects cross-border data transfers depending on where one stand on the globe; in Britain or in the EU,” he said.

By Ali Qassim

With assistance from George R. Lynch in Washington

To contact the reporter on this story: Ali Qassim in London at correspondents@bna.com

To contact the editors responsible for this story: Donald G. Aplin at daplin@bna.com; Daniel R. Stoller at dstoller@bna.com