On April 13, 2016, the Article 29 Working Party, a group consisting of representatives of the European data protection authorities, the European Data Protection Supervisor and the Commission ("Working Party"), published its Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision ("Opinion"). The Opinion highlights many "significant improvements" in the Privacy Shield but also raises a number of concerns and seeks clarifications regarding the framework. The Opinion concludes by urging the Commission to carry out further work on the Privacy Shield to ensure that the final version of the adequacy decision on the Privacy Shield ensures "essentially equivalent" protection for personal data transferred from the European Union to the U.S.

The Working Party’s Opinion is not legally binding on the Commission but will likely be influential.

**Background**

On October 6, 2015, the Court of Justice of the European Union ("CJEU") invalidated the EU-U.S. Safe Harbor in *Case C-362/14 Maximillian Schrems v Data Protection Commissioner* rendering any transfers of personal data from the European Union to the U.S. on the basis of that framework illegal. In the case, the CJEU ruled that the requirement under the EU’s Data Protection Directive 95/46/EC ("Directive") that a third country ensures an *adequate* level of protection to permit data transfers from the EU to such country should be interpreted as "requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental right and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the Directive read in the light of the Charter" (the "essentially equivalent" test).

Following the CJEU’s judgment, the Working Party called on the EU to open negotiations with the U.S. to secure a new framework for transatlantic data transfers by the end of January 2016. On February 2, 2016, the European Commission and the U.S. Department of Commerce reached a political agreement on the Privacy Shield and, then a few weeks later, on February 29, 2016, the European Commission published the documents constituting the new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield, which is intended to replace the now defunct EU-U.S. Safe Harbor.  

---


2 Schrems, paragraph 73.

3 These documents are the Commission Communication COM(2016)117 final, February 29, 2016, a draft adequacy decision and the annexed texts to the adequacy decision.
Procedural Steps

The Privacy Shield will need to be adopted by the College of Commissioners\(^4\) on the basis of the “comitology” procedure pursuant to the Directive. This procedure is composed of various steps identified in the below table.

<table>
<thead>
<tr>
<th>Procedural Step</th>
<th>Timeframe</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication of the draft adequacy decision</td>
<td>February 29, 2016</td>
<td></td>
</tr>
<tr>
<td>Delivery of an opinion by the Working Party</td>
<td>April 13, 2016</td>
<td>The Working Party’s opinion is not legally binding and the Commission is not required to seek a second opinion from the Working Party.</td>
</tr>
<tr>
<td>Delivery of an opinion by the Article 31 Committee(^5)</td>
<td>Committee meetings have been scheduled for April 29, 2016 and May 19, 2016. The vote on the draft adequacy decision is supposed to take place during the latter meeting</td>
<td>The Commission cannot adopt the draft adequacy decision unless the Committee supports it by a qualified majority. If there is a negative vote, the Commission can either re-draft the decision or submit it to the appeal committee for consideration.</td>
</tr>
<tr>
<td>Adoption by the College of Commissioners of the final adequacy decision</td>
<td>The Commission is aiming to adopt the Privacy Shield adequacy decision by June 2016</td>
<td></td>
</tr>
<tr>
<td>Translation and publication of the final adequacy decision</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Working Party Opinion

The Working Party assessed the draft adequacy decision on the Privacy Shield against the applicable data protection framework, including the CJEU’s ruling in Schrems, to determine whether the new framework meets the “essentially equivalent” test, as explained above. The Opinion is divided into two parts: one dealing with the commercial aspects, the other with the

---

\(^4\) The College of Commissioners consists of 28 Commissioners—one from each EU Member State.

\(^5\) Article 31 Committee is an ad hoc comitology committee composed of Member State representatives and chaired by the Commission.
national security, law enforcement and public interest exceptions provided for in the Privacy Shield.

The Opinion is almost 60 pages long and very detailed. The Opinion highlights many “significant improvements” introduced by the new framework compared to the Safe Harbor, such as the insertion of certain key definitions, the procedure for ensuring increased transparency and oversight of the Privacy Shield list and the enhanced data subject rights. It also sets out a number of specific concerns, some of which are less meaningful than others (such as moving language from footnotes to the main text or making it clear in the Privacy Shield that processing of personal data in the EU prior to the transfer to the U.S. is subject the data protection law of the relevant EU Member State). This note focuses on the more significant issues highlighted by the Opinion.

General Remarks

The below table summarizes the main concerns and recommended actions the Working Party highlights as applicable to the Privacy Shield framework as a whole.

<table>
<thead>
<tr>
<th>Concern</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall lack of clarity with the architecture of the documents establishing the Privacy Shield and the terminology used across those documents</td>
<td>The Working Party recommends that the Privacy Shield is accompanied by a glossary that sets out clear definitions for the terms used in the framework and it is ensured that those terms are used consistently across the documents.</td>
</tr>
<tr>
<td>Inability to carry out a complete analysis of the U.S. legal framework in which the Privacy Shield operates</td>
<td>The Commission should have provided an adequacy report setting out a comprehensive assessment of the national laws and international commitments of the U.S., as is the typical practice when the Commission adopts adequacy decisions.</td>
</tr>
<tr>
<td>Lack of reference to the General Data Protection Regulation (“GDPR”)</td>
<td>The Privacy Shield should include an express reference to a review mechanism that will permit the framework to be adjusted to take into account the higher level of protection required under the GDPR once it comes into effect in 2018.</td>
</tr>
<tr>
<td>Unclear joint review process6</td>
<td>The Commission should clarify the modalities for the joint annual review of the Privacy Shield, including the details around the report setting out the findings of the review and the modalities of the involvement of the national data protection authorities</td>
</tr>
</tbody>
</table>

6 The joint review refers to the process by which the European Commission and the U.S. administration review the practical application of the Privacy Shield on an annual basis.
Data Privacy and Cybersecurity

Commercial Aspects

The Working Party identifies the following main concerns with the commercial aspects of the Privacy Shield:

- **Some of the key data protection principles set out in the EU’s data protection law are not sufficiently reflected in the Privacy Shield.** In particular, there is no clear obligation on organizations to delete personal data once it is no longer required for the purpose for which it was collected, hence making it possible for organizations to retain the data indefinitely. Similarly, the application of the purpose limitation principle under the Privacy Shield is not clear; the Working Party draws particular attention to the inconsistent terms used in the “Purpose Limitation” and “Choice” principles regarding the purposes for which the transferred personal data may be used. The Working Party also notes that the Privacy Shield should include restrictions on automated decision-making and should provide data subjects with a general right to object similar to that set out in the Directive.

- **The onward transfer principle is not sufficiently robust.** The Working Party notes that every Privacy Shield organization wishing to onward transfer personal data to a third country should be obliged to assess any mandatory requirements of the third country’s national legislation prior to the transfer. If that assessment identifies a risk of “substantial adverse effect” on the level of protection provided by the Privacy Shield, the onward transfer should not normally go ahead. Additional clarifications are also needed to ensure that the scope, the purpose limitation and the guarantees applying to onward transfers to processors (Agents) are sufficient.

- **The Privacy Shield does not sufficiently address its application to self-certified organizations acting as processors.** The Working Party notes that it is difficult to determine which Privacy Shield principles apply (and how) to those organizations that certify to the Privacy Shield but process the transferred personal data as processors and notes that the Privacy Shield should contain specific rules in those circumstances to ensure that the U.S.-based processor only processes personal data pursuant to the controller’s instructions.

- **Redress mechanisms provided to data subjects are too complex and ineffective.** The Working Party seeks further clarification on the overall architecture of the recourse mechanisms offered to EU data subjects (i.e., raising concerns with the self-certified company, via an independent dispute resolution body, to the Federal Trade Commission, and via binding arbitration) and suggests that DPAs should act as their first point of contact. The DPAs should also have the option to act as intermediaries for the data subjects or to act on their behalf.

- **Clarifications are required to the application of the Privacy Shield principles to human resources and clinical data.** In particular, the Working Party notes that some of the proposed exceptions applicable to human resources (“HR”) data (e.g., the exception to the Access principle and to the obligation to enter into a contract with a third-party controller for HR data where it relates to occasional employment-related operations) should be removed. Further, the Working Party emphasizes that key-coded data constitutes personal data and, hence, if transfers of such data are not covered by the Privacy Shield as suggested by the draft adequacy decision, such
transfers must be covered by one of the other transfer mechanisms, such as the European Commission Standard Contractual Clauses (“SCCs”).

**National Security Elements**

The Opinion is accompanied by Working Document 01/2016 setting out “European Essential Guarantees” (discussed in more detail in the next section), which sets out the European standards applicable to state surveillance activities. The Opinion uses the European Essential Guarantees as part of the assessment of whether the Privacy Shield exceptions for national security, law enforcement and public interest are compliant with European law.

The Working Party highlights the following main concerns with respect to the national security elements of the Privacy Shield:

- **The Privacy Shield leaves it open for the U.S. government to carry out indiscriminate and massive data collection.** While the Working Party notes that the U.S. signals intelligence activities are conducted on the basis of an accessible legal framework, that framework leaves it open for the U.S. government to engage in bulk collection of data. And, while there are rules that limit the purposes for which the signals intelligence collected in bulk can be used, those purposes are too broadly worded and, in any case, do not prevent the collection of the data in bulk. Hence, the Working Party concludes that concerns regarding the necessity and proportionality of the collection and use of intelligence data remain.

- **There are concerns over the independency and effective powers of the Ombudsperson.** The Working Party is particularly concerned that the Privacy Shield does not create specific criteria for the dismissal of the Ombudsperson, hence potentially undermining its independency. Further, the Working Party notes that it is unclear whether the Ombudsperson would have direct access to the data in question to carry out its investigation or would be required to rely on the reports from other U.S. government officials. Finally, it is unclear how the Ombudsperson would be able to order non-compliance to be remedied.

- **There are insufficient effective remedies available to individuals.** In particular, the Working Party emphasizes that EU data subjects will in practice struggle to establish standing before U.S. courts and that non-U.S. citizens located outside the country do not benefit from the protection of the Fourth Amendment of the U.S. Constitution, which protects U.S. citizens against unreasonable searches and seizures.

- **The lack of information on U.S. laws governing law enforcement access to data makes it impossible for the Working Party to finalize its assessment.** According to the Working Party, the U.S. system governing investigative tools of law enforcement is complex and, hence, further information is required to carry out a comprehensive assessment of the accessibility, foreseeability, necessity and proportionality of the applicable U.S. rules.

---

7 The Ombudsperson is the new oversight mechanism the U.S. government has established to deal with data subjects’ complaints about U.S. law enforcement access to their data. The Ombudsperson is appointed by the Secretary of State to act as a “Senior Coordinator for International Information Technology Diplomacy” (Senior Coordinator) “to … serve as a point of contact for foreign governments who wish to raise concerns regarding signals intelligence activities conducted by the United States.” The current Under Secretary C. Novelli is serving as the Senior Coordinator.
European Essential Guarantees

As noted above, the Opinion is accompanied by a Working Document that sets out standards for assessing whether a national law governing state surveillance activities can be regarded as a justifiable interference to fundamental rights in a democratic society (so-called “European Essential Guarantees”). The Working Party has developed these standards on the basis of the jurisprudence of the CJEU and the European Court of Human Rights (“ECHR”) concerning fundamental rights and freedoms, including the right to private life and to data protection.

The Working Document identifies the following four European Essential Guarantees:

**Guarantee A:** Processing should be based on clear, precise and accessible rules.

The interference with the individuals’ rights must be foreseeable and, hence, there must be rules that are clear, detailed and publicly available so that individuals have an adequate indication of the circumstances in which surveillance activities may take place.

**Guarantee B:** Processing should be necessary and proportional with regard to the legitimate objectives pursued.

There should be an objective criterion to limit the collection and access to data (although the courts have not taken a final position on the legality of massive and indiscriminate collection of personal data and its subsequent use).

**Guarantee C:** There should be an independent oversight mechanism.

The oversight system, which should be a judge or another independent body, should be sufficiently independent from the executive and of the surveillance authorities and must have sufficient powers and competence to carry out an effective control.

**Guarantee D:** Individuals should have access to effective remedies.

Individuals must have an effective remedy to satisfy their rights when they think they have not been respected.

Importantly, the Working Party emphasizes that the European Essential Guarantees apply equally to surveillance activities carried out by foreign and EU governments. The Working Party further notes that it does not “maintain a double standard” and, hence, has on several occasions called on EU Member States to ensure that their surveillance laws are compliant with the case law of the CJEU and the ECHR.

**What Is the Impact?**

The impact of the Working Party’s Opinion on the future transfers of personal data to the U.S. will only become apparent once the Commission adopts the final adequacy decision on the Privacy Shield, hopefully by June. Even then, there is a risk that the validity of the Privacy Shield may be challenged before the CJEU. During the Working Party’s press conference on the Opinion, the chainwoman of the Working Party, CNIL President Falque-Pierrotin, did not exclude the possibility of a judicial challenge of the Privacy Shield if the
Commission ignores its concerns regarding the Privacy Shield set out in the Opinion. This means that organizations wishing to rely on the Privacy Shield to transfer personal data from the EU to the U.S. may face legal uncertainty even after the adoption of the framework.

The Working Party’s Opinion does not have a direct impact on the validity of the other transfer mechanisms under the Directive, however. In fact, Ms. Falque-Pierrotin confirmed during the Working Party’s press conference on the Opinion that SCCs and Binding Corporate Rules (“BCRs”) will continue to be valid mechanisms to transfer data outside the EU. That said, the Working Party left it open whether it will review those transfer mechanisms once the Commission has adopted the final adequacy decision on the Privacy Shield. Importantly, the Working Party states in the European Essential Guarantees document that those guarantees apply to all data transfers, whether carried out on the basis of Article 25 or 26 of the Directive, which cover international transfers not only on the basis of adequacy decisions, but also based on statutory derogations and safeguards, such as SCCs and BCRs. This implies the possibility that the Working Party may carry out a similar assessment of those transfer mechanisms against the European Essential Guarantees as that done with respect to the Privacy Shield, potentially resulting in recommendations for additional guarantees for those mechanisms.

**Next Steps**

The Working Party Opinion is not legally binding, however, European Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, has indicated that the Commission will work to include the recommendations raised by the Working Party in the draft adequacy decision.

It is likely that some of the changes suggested by the Working Party should be relatively easy to implement, especially those that are more focused on the format than the substance or those where the Commission and the U.S. likely already have a common understanding (such as some of the defined terms used in the Privacy Shield). However, some of the main concerns identified by the Working Party will likely take more time to implement or may even require the re-opening of the negotiations with the U.S. government.

That said, it may be sufficient if the European Commission and the U.S. government provide additional clarifications and guarantees in writing without having to re-open the text of the Privacy Shield. In particular, the chairwoman of the Working Party explained during the press conference on the Opinion that the Commission and the U.S. government had provided many clarifications to the Working Party during several meetings held as part of the Working Party’s review of the Privacy Shield. The chairwoman confirmed that many of the Working Party’s concerns with the Privacy Shield would be addressed if the Commission and the U.S. government are willing to put those clarifications in writing. In addition, the Commission seems to have taken steps to provide additional clarifications following the Working Party’s Opinion: Commissioner Jourová released a letter on the role, powers and independence of the Ombudsperson on April 14, 2016, apparently aiming to address some of the Working Party’s related concerns.8

It is also possible that not all of the Working Party’s concerns need to be addressed before the final adequacy decision is adopted but may be dealt with later. In particular, the Working Party notes that it may be possible to finalize its assessment of the U.S. laws and rules

---

governing law enforcement access to data against the European Essential Guarantees during the annual review of the Privacy Shield. Further, the Working Party’s conclusions and recommendations in the Opinion seem to indicate that the Working Party’s concerns on data retention, the Ombudsperson, and bulk surveillance are more critical than some of the other concerns raised in the Opinion, hence implying that, if concerns are addressed prior to the adoption of the final adequacy decision, it may be possible to deal with the others at a later stage.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Privacy and Data Security team:

Jetty Tielemans  
+32 2 549 52 52  
htielemans@cov.com

Monika Kuschewsky  
+32 2 549 52 49  
mkuschevesky@cov.com

Helena Marttila-Bridge  
+44 20 7067 2042  
hmarttila-bridge@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

In an increasingly regulated world, Covington & Burling LLP provides corporate, litigation, and regulatory expertise to help clients navigate through their most complex business problems, deals and disputes. Founded in 1919, the firm has more than 800 lawyers in offices in Beijing, Brussels, Los Angeles, London, New York, San Francisco, Seoul, Shanghai, Silicon Valley, and Washington.

This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.