March 1, 2016

3things

The 3 things you need to know about...

Transatlantic Data Flows in 2016 and Beyond

Summary

#1 - The legal construct around European Union (EU) to U.S. personal data transfers has become uncertain as new European privacy regulations emerge.

#2 - The General Data Protection Regulation (GDPR) and Network and Information Security Directive (NIS) will likely have a larger influence and longer term impact than Privacy Shield on how U.S. companies with EU operations define and execute on their strategy.

#3 - Companies should be working across their organization to baseline their potential exposure under GDPR, NIS and Privacy Shield - the countdown to compliance starts now.

The Three Things

#1 - The legal construct around European Union (EU) to U.S. personal data transfers has become uncertain as new European privacy regulations emerge.

On February 2, 2016, negotiators from the European Commission and U.S. Department of Commerce struck an agreement on a new transatlantic data flow framework dubbed the "EU-U. S. Privacy Shield" to replace the defunct Safe Harbor program.[1] Following the Court Justice of the European Union (CJEU) decision to invalidate Safe Harbor last October, thousands of active U.S. Safe Harbor registrants have been without an approved mechanism to transfer the personal data of EU citizens to the U.S.

Negotiators on both sides of the Atlantic scrambled to strike a deal by the January 31 deadline imposed by the committee of European Data Protection Authorities (DPAs) known as the Article 29 Working Party (WP29).[2] As a result, the negotiation of Privacy Shield was a hurried effort relative to the two years spent on the development of the Safe Harbor agreement, raising questions about the breadth of its support across the EU and its long-term viability.

Even with the negotiators' agreement, the Privacy Shield will face a series of challenges along the road to implementation. The European Commission and U.S. Department of Commerce released the the detailed text of the Privacy Shield agreement and a draft "adequacy decision" on February 29. WP29 will review the agreement in a special session to determine if it provides adequate protection under EU law prior to a final decision. In addition, the agreement will likely face a challenge by the CJEU and could be invalidated under the same rationale as Safe Harbor.

Adding to the complexity, the European Parliament and European Council agreed on a final draft of the General Data Protection Regulation (GDPR) in December. This landmark piece of legislation will be phased into effect over the next two years, with initial enforcement of the regulation to take effect in 2018. The approval of the GDPR marks the latest effort to give EU citizens a greater say over how their digital information is collected and managed. This overhaul of EU privacy rules will present compliance challenges for businesses that hold or use personal data of EU citizens both inside and outside the EU. Absent necessary controls, privacy violations could lead to EU enforcement actions reaching up to 4% of global revenue.[3]

#2 - The General Data Protection Regulation (GDPR) and Network and Information Security Directive (NIS) will likely have a larger influence and longer term impact on how U.S. companies with EU operations define and execute on their strategy.

Firms with European operations should consider the GDPR and the NIS as two sides of the same coin. The approval of the Privacy Shield program may be beneficial to former Safe Harbor registrants should it come to fruition. However, the GDPR and the NIS Directive have significant implications for U.S. companies with operations in the EU.

The GDPR is the legal side of the coin and establishes many of the legal, contractual, and operational requirements under which non-EU firms must operate to establish EU-level protection for the citizens of member jurisdictions. GDPR compliance requirements include an appointed privacy officer, privacy by design and default in products and services, the right to be forgotten, additional privacy impact assessments, and encryption of sensitive personal data at rest.

The NIS Directive is the technical side of the coin and establishes minimum information security and privacy breach incident notification requirements for operators of "essential services" including certain digital infrastructure, which covers online marketplaces, online search engines, and cloud computing services. Social networks do not appear to be covered under the NIS at this time.

In addition to the compliance challenges, companies need to consider the strategic and operational impacts that will arise as a result of the new regulations. Potential business impacts will vary depending on the products, services, and solutions offered, including:

Strategic	*Operational*
• **Go-to-market plans:** New privacy compliance requirements could present barriers for companies entering EU markets or scaling existing operations. • **Privacy by design and default:** Data protection safeguards required to be designed into new and existing products and services (e.g., cloud services, networking equipment) to protect EU citizen privacy. • **Organizational footprint:** Existing and planned data center locations could be subject to GDPR and data transfer compliance requirements.	• **Customer management:** Collection, storage and transfer of EU customer data through marketing and general customer management operations. • **Human resource management:** Collection, storage and transfer of EU citizen data for recruiting and managing company talent (e.g., payroll, HR software-as-service) • **Contract management:** Contractual language among vendors/supply chain partners as well as corporate structures to clarify roles of data controllers and data processors

Although GDPR and NIS will likely have a larger impact on companies' long term operations, firms that elect to implement Privacy Shield have to consider the immediate impact on their business. U.S. companies can expect more regulatory scrutiny and an increased burden of proof for compliance as the Federal Trade Commission (FTC) takes on a more active role in monitoring registrants. In concert with the FTC oversight, the Judicial Redress Act, which was signed into law in February, provides a pathway for EU citizens to take up a cause of action against a US firm. The

Judicial Redress Act, combined with the Privacy Shield and/or the GDPR will enable individual Europeans to make privacy complaints against U.S. companies.

#3 - U. S. companies should be working across their organization to baseline their potential exposure under GDPR, NIS and Privacy Shield - the countdown to compliance starts now.

U.S. companies must understand and document how EU citizens' personal data is transferred, stored, and utilized throughout their organization. While WP29 may not pursue coordinated enforcement action, some EU DPAs - most notably Germany and Spain - indicated that they may move against U.S. companies before the finalization of the Privacy Shield. The French legislature is also considering a new law that would codify key parts of the GDPR with a more immediate entry-into-force date.

A number of the key provisions of Privacy Shield overlap with GDPR requirements. As a starting point, all U.S. companies with EU operations should address the apparent overlaps as details of the Privacy Shield are reviewed by EU regulators:

1. *European customers and citizens will have the right to file individual complaints* - DPAs have an obligation to investigate complaints. Privacy Shield will give EU citizens a number of new avenues to pursue complaints including a dedicated team with new resources and an independent Ombudsman within the Department of State.

2. *Binding Corporate Rules and Model Contracts are the only acceptable data transfer mechanisms* - Because the timing of Privacy Shield is unclear, U.S. companies handling EU citizen data should continue to implement Binding Corporate Rules and Model Contract Clauses. WP29 confirmed the short-term validity of these alternative methods, but U.S. companies should continue to monitor the legality of these alternatives following the implementation of Privacy Shield.

3. *Law enforcement and national security organizations are subject to new restrictions* - Following the implementation of GDPR and Privacy Shield, law enforcement will only be able to access EU citizen personal information "to the extent necessary." Without further guidance, U.S. firms will face significant compliance challenges when responding to law enforcement requests.

Execution of a plan to address the three considerations above is only the beginning for U.S. companies that wish to navigate this regulatory change successfully, and position themselves at a competitive advantage. Firms that choose to make an investment in their technology and privacy infrastructure now will be ahead of their competitors, and could avoid inquiries from regulators and potentially costly fines. Companies should map all of their EU data flows and establish a baseline of their exposure to the new regulations. With that exposure in mind, they should conduct a detailed risk assessment, examining the adequacy of their privacy and data protection controls. Using the risk assessment, they can then develop and execute on a roadmap to achieve compliance and address the business impacts associated with GDPR, NIS, and Privacy Shield.

Privacy compliance issues arising from the GDPR and Privacy Shield for entities with a footprint in the EU will be time consuming and costly to address. Accordingly, 2016 may prove to be a challenging year as firms organize and mobilize their data compliance response plans and policies.

Endnotes

1. Source: Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment <http://ec.europa.eu/justice/dataprotection/article29/pressmaterial/pressrelease/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf>
2. Source: Article 29 Data Protection Working Party. Opinion on Schrems decision. October 16, 2015. <http://ec.europa.eu/justice/dataprotection/article29/pressmaterial/pressrelease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf>
3. Source: European Commission press release, "Agreement on Commission's EU data protection reform will boost Digital Single Market" December 15, 2015. <http://europa.eu/rapid/pressrelease_IP156321_en.htm>
4. Source: Commission welcomes agreement to make EU online environment more secure <http://europa.eu/rapid/pressrelease_IP156270_en.htm>
5. Source: EU-U.S. Privacy Shield Fact Sheet <https://www.commerce.gov/news/factsheets/2016/02/euusprivacyshield>
6. Source: General Data Protection Regulation <http://www.haerting.de/sites/default/files/pdfs/proposaleudatapregulationfinalcompromise151216.pdf>
7. PwC Financial Crimes Observer: Cyber: Global data transfer still in disarray <https://www.pwc.com/us/en/financialservices/financialcrimes/publications/assets/euusprivacyshield2016.pdf>

Additional information

For additional information about this topic and how PwC can help, please contact:

Kayvan Shahabi

U.S. Advisory Technology Industry Leader
(408) 871-5724
kayvan.shahabi@pwc.com

Joe Atkinson

US Advisory Entertainment, Media & Communications Leader
(267) 330-2494
joseph.atkinson@pwc.com

David Sapin

TICE Risk & Regulatory Leader
(202) 756-1737
david.sapin@pwc.com

Mark Lobel

TICE Advisory Cybersecurity & Privacy Leader
(646) 471-5731
mark.a.lobel@pwc.com

Aaron Weller

Cybersecurity & Privacy Managing Director
(206) 398-3497
aaron.weller@pwc.com

Jacky Wagner

Cybersecurity & Privacy Managing Director
(646) 471-5644
jacqueline.t.wagner@pwc.com

Contributing authors: Marc Mazzie, Scott Margolis, Christopher Caulfield, Peter Lester

3things is a publication of PwC's TICE Advisory Risk and Regulatory practice and is intended to highlight 3 key takeaways from evolving risk and regulatory issues impacting the Technology, Communications, Media & Entertainment and Hospitality, Gaming & Leisure sectors. Companies in these rapidly evolving industries face increasing market and competitive risks, as well as other internal and financial risks from the challenges of managing their complex and often global businesses. They are also facing an uncertain regulatory environment, as regulators across the globe grapple with how to effectively implement their policy objectives in an era of unprecedented technological change. The TICE Risk and Regulatory team brings a combination of deep industry expertise and an understanding of the evolving regulatory environment to help our clients in these sectors navigate the risk and regulatory complexities of running their business and executing on their strategies.